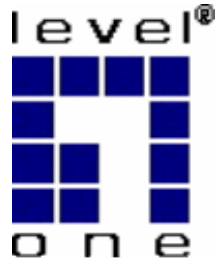

LevelOne

WBR-6000
N_One Wireless Broadband Router

User Manual

V1.0.0-0705

Table of Contents

CHAPTER 1 INTRODUCTION 3
- Wireless Broadband Router Features 3
- Package Contents 6
- Physical Details 7

CHAPTER 2 INSTALLATION 9
- Requirements 9
- Procedure 9

CHAPTER 3 SETUP 11
- Overview 11
- Configuration Program 12
- Setup Wizard 13
- Home Screen 16
- LAN Screen 18
- Wireless Screen 20
- Wireless Security 23
- Password Screen 27

CHAPTER 4 PC CONFIGURATION 28
- Overview 28
- Windows Clients 28
- Macintosh Clients 36
- Linux Clients 36
- Other Unix Systems 36
- Wireless Station Configuration 37

CHAPTER 5 OPERATION AND STATUS 38
- Operation 38
- Status Screen 38
- Connection Status - PPPoE 41
- Connection Status - PPTP 42
- Connection Status - L2TP 43
- Connection Status - Telstra Big Pond 45
- Connection Details - SingTel RAS 46
- Connection Details - Dynamic IP Address 48
- Connection Details - Fixed IP Address 50

CHAPTER 6 ADVANCED FEATURES 51
- Overview 51
- Internet 51
- Access Control 54
- Dynamic DNS (Domain Name Server) 57
- Firewall Rules 59
- Firewall Services 64
- Virtual Servers 65
- Options 69
- Port Trigger 70
- Schedule 71

CHAPTER 7 ADVANCED ADMINISTRATION 73
- Overview 73
- PC Database 74
- Diagnostics 76
- Config File 78
- Logs 79
- Remote Administration 80

Upgrade Firmware **82**
APPENDIX A TROUBLESHOOTING **83**
Overview **83**
General Problems **83**
Internet Access **83**
Wireless Access **84**
APPENDIX B ABOUT WIRELESS LANS **86**
Modes **86**
BSS/ESS **86**
Channels **86**
WEP **87**
WPA-PSK **87**
Wireless LAN Configuration **87**
APPENDIX C SPECIFICATIONS **89**
Multi-Function Wireless Broadband Router **89**
Wireless Interface **89**
Regulatory Approvals **90**

Chapter 1
Introduction

This Chapter provides an overview of the Wireless Broadband Router's features and capabilities.

Congratulations on the purchase of your new Wireless Broadband Router. The Wireless Broadband Router is a multi-function device providing the following services:

- ***Shared Broadband Internet Access*** for all LAN users.
- ***4-Port Switching Hub*** for 10BaseT or 100BaseT connections.

Figure 1: Wireless Broadband Router

Wireless Broadband Router Features

The Wireless Broadband Router incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

Internet Access Features

- ***Shared Internet Access.*** All users on the LAN or WLAN can access the Internet through the Wireless Broadband Router, using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- ***DSL & Cable Modem Support.*** The Wireless Broadband router has a 10/100BaseT Ethernet port for connecting a DSL or Cable Modem. All popular DSL and Cable Modems are supported. SingTel RAS and Big Pond (Australia) login support is also included.
- ***PPPoE, PPTP, SingTel RAS and Telstra Big Pond Support.*** The Internet (WAN port) connection supports PPPoE (PPP over Ethernet), PPTP (Peer-to-Peer Tunneling Protocol), L2TP, SingTel RAS and Telstra Big Pond (Australia), as well as "Direct Connection" type services. Unnumbered IP with PPPoE is also supported.
- ***Fixed or Dynamic IP Address.*** On the Internet (WAN port) connection, the Wireless Broadband Router supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

Advanced Internet Functions

- ***URL Filter.*** Use the URL Filter to block access to undesirable Web sites by LAN users.
- ***DMZ.*** For each WAN (Internet) IP address allocated to you, one (1) PC on your local LAN can be configured to allow unrestricted 2-way communication with Servers or individual users on the Internet. This provides the ability to run programs which are incompatible with Firewalls.
- ***Access Control.*** Using the Access Control feature, you can determine which Internet services are available to LAN users.

- ***Dynamic DNS Support.*** DDNS, when used with the Virtual Servers feature, allows users to connect to Servers on your LAN using a Domain Name, even if you have a dynamic IP address which changes every time you connect.
- ***Firewall.*** As well as the built-in firewall to protect your LAN, you can define Firewall Rules to determine which incoming and outgoing traffic should be permitted.
- ***Firewall Services.*** Applications which use non-standard connections or port numbers are normally blocked by the Firewall. The ability to define and allow such applications is provided, to enable such applications to be used normally.
- ***Port Trigger.*** This feature allows you to use Internet applications which normally do not function when used behind a firewall.
- ***Scheduling.*** Both the URL Filter and Firewall rules can be scheduled to operate only at certain times. This provides great flexibility in controlling Internet -bound traffic.
- ***Virtual Servers.*** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- ***VPN Pass through Support.*** PCs with VPN (Virtual Private Networking) software using PPTP, L2TP and IPSec are transparently supported - no configuration is required.
- ***Logs.*** Define what data is recorded in the Logs, and optionally send log data to a Syslog Server. Log data can also be E-mailed to you.

Wireless Features

- ***Standards Compliant.*** The Wireless Broadband Router complies with the IEEE802.11g (DSSS) specifications for Wireless LANs.
- ***Supports Pre-N Wireless Stations.*** The 802.11n Draft standard provides for backward compatibility with the 802.11b standard, so both 802.11b and 802.11g Wireless stations can be used simultaneously.
- ***Speeds up to 300Mbps.*** All speeds up to the draft 802.11n maximum of 300Mbps are supported.
- ***WEP support.*** Support for WEP (Wired Equivalent Privacy) is included. Key sizes of 64 Bit and 128 Bit are supported. WEP encrypts any data before transmission, providing protection against snoopers.
- ***WPA-PSK support.*** Like WEP, WPA-PSK encrypts any data before transmission, providing protection against snoopers. The WPA-PSK is a later standard than WEP, and provides both easier configuration and greater security than WEP.
- ***WPA2-PSK support.*** WPA2-PSK is also supported. WPA2-PSK uses the extremely secure AES encryption method.
- ***Wireless MAC Access Control.*** The Wireless Access Control feature can check the MAC address (hardware address) of Wireless stations to ensure that only trusted Wireless Stations can access your LAN.
- ***Simple Configuration.*** If the default settings are unsuitable, they can be changed quickly and easily.

LAN Features

- ***4-Port Switching Hub.*** The Wireless Broadband Router incorporates a 4-port 10/100BaseT switching hub, making it easy to create or extend your LAN.

- ***DHCP Server Support.*** **D**ynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The Wireless Broadband Router can act as a **DHCP Server** for devices on your local LAN and WLAN.

Configuration & Management

- ***Configuration File Upload/Download.*** Save (download) the configuration data from the Wireless Broadband Router to your PC, and restore (upload) a previously-saved configuration file to the Wireless Broadband Router.
- ***Remote Management.*** The Wireless Broadband Router can be managed from any PC on your LAN or Wireless LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.
- ***Diagnostics.*** You can use the Wireless Broadband Router to perform a *Ping* or *DNS lookup*.
- ***UPnP Support.*** UPnP (Universal Plug and Play) allows automatic discovery and configuration of the Wireless Broadband router. UPnP is by supported by Windows ME, XP, or later.

Security Features

- ***Password - protected Configuration***. Password protection is provided to prevent unauthorized users from modifying the configuration data and settings.
- ***Wireless LAN Security***. WPA/WPA2-PSK, WEP and Wireless access control by MAC address are also supported. The MAC-level access control feature can be used to prevent unknown wireless stations from accessing your LAN.
- ***NAT Protection.*** An intrinsic side effect of NAT (Network Address Translation) technology is that by allowing all LAN users to share a single IP address, the location and even the existence of each PC is hidden. From the external viewpoint, there is no network, only a single device - the Wireless Broadband Router.
- ***Firewall.*** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.
- ***Protection against DoS attacks.*** DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The Wireless Broadband Router incorporates protection against DoS attacks.

Package Contents

The following items should be included. If any of these items are damaged or missing, please contact your dealer immediately.

- WBR-6000
- Cat.5 Cable
- Power Adapter
- Quick Installation Guide
- CD Manual

If any of the above items are damaged or missing, please contact your dealer immediately.

Physical Details

Front-mounted LEDs

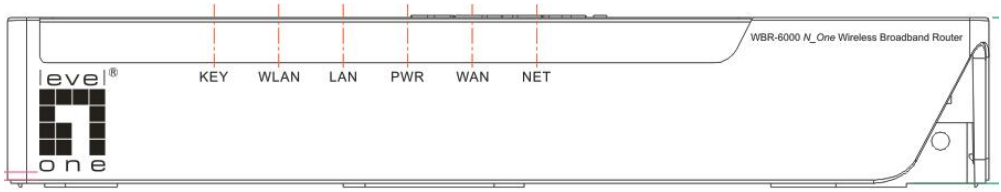

Figure 2: Front Panel

KEY

On - Wireless security is On.

Off - Wireless security is Off.

WLAN

On - Wireless enabled.

Off - No Wireless connections currently exist.

Flashing - Data is being transmitted or received via the Wireless access point. This includes "network traffic" as well as user data.

LAN

- **On** - Corresponding LAN (hub) port is active.
- **Off** - No active connection on the corresponding LAN (hub) port.
- **Flashing** - Data is being transmitted or received via the corresponding LAN (hub) port.

PWR

On - Power on.

Off - No power.

Flashing - This LED blinks during start up, and during a Firmware Upgrade.

WAN

On - Connection to the modem attached to the WAN (Internet) port is established.

Flashing - Data is being transmitted or received via the WAN port.

NET

On - Internet connection is available.

Off - No Internet connection available.

Flashing - Data is being transmitted or received via the ADSL connection.

Rear Panel

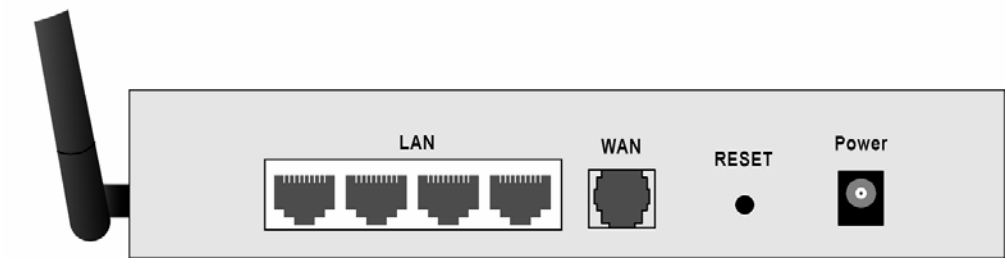

Figure 3: Rear Panel

10/100BaseT LAN connections

Use standard LAN cables (RJ45 connectors) to connect your PCs to these ports.

Note:

Any LAN port on the Wireless Broadband Router will automatically function as an "Uplink" port when required. Just connect any port to a normal port on the other hub, using a standard LAN cable.

WAN port (10/100BaseT)

Connect the DSL or Cable Modem here. If your modem came with a cable, use the supplied cable. Otherwise, use a standard LAN cable.

Reset Button

This button has two (2) functions:

- **Reboot**. Press and hold the Reset Button for five (5) seconds and released, the Wireless Broadband router will reboot (restart).
- **Clear All Data**. This button can also be used to clear ALL data and restore ALL settings to the factory default values.

To Clear All Data and restore the factory default values:

- Power ON, push and hold the reset button for 10 sec.

Release the Reset Button. The Wireless Broadband router will reboot and now is using the factory default values.

Power port

Connect the supplied power adapter here.

Chapter 2
Installation

This Chapter covers the physical installation of the Wireless Broadband Router.

Requirements

- Network cables. Use standard 10/100BaseT network (UTP) cables with RJ45 connectors.
- TCP/IP protocol must be installed on all PCs.
- For Internet Access, an Internet Access account with an ISP, and a DSL connection.
- To use the Wireless Access Point, all Wireless devices must be compliant with the IEEE 802.11g, IEEE 802.11b or IEEE 802.11n Draft specifications.

Procedure

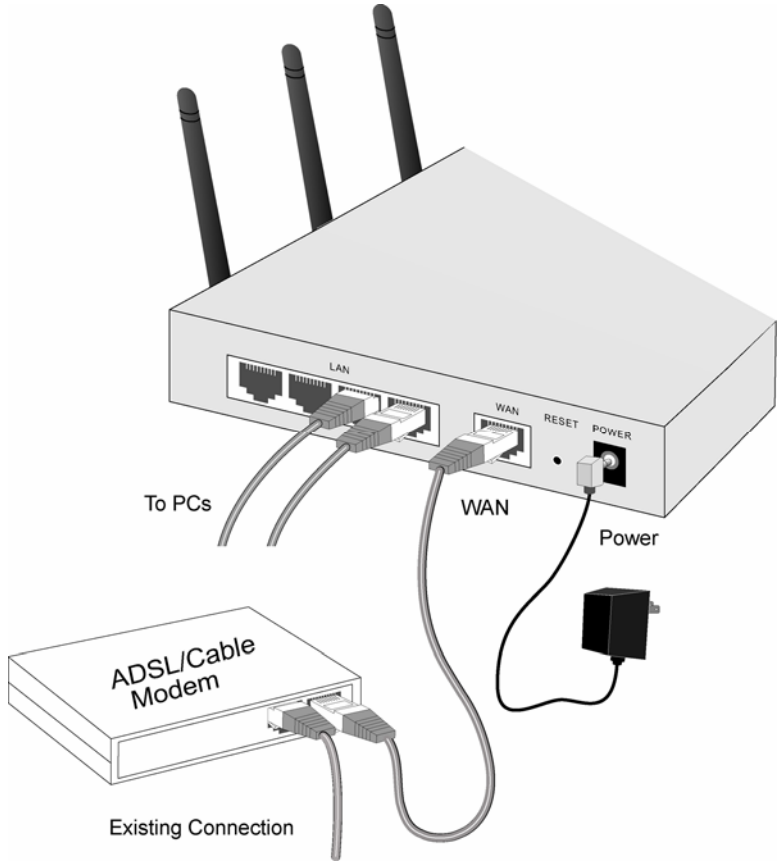

Figure 4: Installation Diagram

1. Choose an Installation Site

Select a suitable place on the network to install the Wireless Broadband Router.

For best Wireless reception and performance, the Wireless Broadband Router should be positioned in a central location with minimum obstructions between the Wireless Broadband Router and the PCs.

Also, if using multiple Access Points, adjacent Access Points should use different Channels.

2. Connect LAN Cables

Use standard LAN cables to connect PCs to the Switching Hub ports on the Wireless Broadband Router. Both 10BaseT and 100BaseT connections can be used simultaneously.

If required, connect any port to a normal port on another Hub, using a standard LAN cable. Any LAN port on the Wireless Broadband Router will automatically function as an "Uplink" port when required.

3. Connect WAN Cable

Connect the DSL or Cable modem to the WAN port on the Wireless Broadband router. Use the cable supplied with your DSL/Cable modem. If no cable was supplied, use a standard cable.

4. Power Up

Connect the supplied power adapter to the Wireless Broadband Router. Use only the power adapter provided. Using a different one may cause hardware damage.

5. Check the LEDs

- The *PWR* LED should be ON.
- For LAN (PC) connection, the LAN LED should be ON (provided the PC is also ON.)
- The *WLAN* LED should be ON if wireless clients are connected.
- The *WAN* LED should be ON if DSL or Cable modem is power ON.
- The *Net* LED may be OFF. After Setup Wizard configuration, it should come ON.

For more information, refer to *Front-mounted LEDs* in Chapter 1.

Chapter 3
Setup

This Chapter provides Setup details of the Wireless Broadband Router.

Overview

This chapter describes the setup procedure for:

- Internet Access
- LAN configuration
- Wireless setup
- Assigning a Password to protect the configuration data.

PCs on your local LAN may also require configuration. For details, see *Chapter 4 - PC Configuration*.

Other configuration may also be required, depending on which features and functions of the Wireless Broadband Router you wish to use. Use the table below to locate detailed instructions for the required functions.

To Do this:	**Refer to:**
Configure PCs on your LAN.	Chapter 4: PC Configuration
Check Wireless Broadband Router operation and Status.	Chapter 5: Operation and Status
Use any of the following Advanced features: • Internet (DMZ, URL Filter) • Access Control • Dynamic DNS • Firewall Rules • Firewall Services • Virtual Servers • Options • Schedule	Chapter 6: Advanced Features
Use any of the following Administration Configuration settings or features: • PC Database • Diagnostics • Config File • Logs • Remote Admin • Upgrade Firmware	Chapter 7 Advanced Administration

Configuration Program

The Wireless Broadband Router contains an HTTP server. This enables you to connect to it, and configure it, using your Web Browser. **Your Browser must support JavaScript**.

The configuration program has been tested on the following browsers:

- Netscape 7.1 or later.
- Mozilla 1.6 or later
- Internet Explorer V5.5 or later

Preparation

Before attempting to configure the Wireless Broadband Router, please ensure that:

- Your PC can establish a physical connection to the Wireless Broadband Router. The PC and the Wireless Broadband Router must be directly connected (using the Hub ports on the Wireless Broadband Router) or on the same LAN segment.
- The Wireless Broadband Router must be installed and powered ON.
- If the Wireless Broadband Router's default IP Address (192.168.0.1) is already used by another device, the other device must be turned OFF until the Wireless Broadband Router is allocated a new IP Address during configuration.

Using your Web Browser

To establish a connection from your PC to the Wireless Broadband Router:

1. After installing the Wireless Broadband Router in your LAN, start your PC. If your PC is already running, restart it.
2. Start your WEB browser.
3. In the *Address* box, enter "HTTP://" and the IP Address of the Wireless Broadband Router, as in this example, which uses the Wireless Broadband Router's default IP Address:

   HTTP://192.168.0.1
4. When prompted for the User name and Password, enter values as follows:
   - User name admin
   - Password password

If you can't connect

If the Wireless Broadband Router does not respond, check the following:

- The Wireless Broadband Router is properly installed, LAN connection is OK, and it is powered ON. You can test the connection by using the "Ping" command:
  - Open the MS-DOS window or command prompt window.
  - Enter the command:
    ping 192.168.0.1
    If no response is received, either the connection is not working, or your PC's IP address is not compatible with the Wireless Broadband Router's IP Address. (See next item.)
- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.0.2 to 192.168.0.254 to be compatible with the Wireless Broadband Router's default IP Address of 192.168.0.1. Also, the *Network Mask* must be set to 255.255.255.0. See *Chapter 4 - PC Configuration* for details on checking your PC's TCP/IP settings.
- Ensure that your PC and the Wireless Broadband Router are on the same network segment. (If you don't have a router, this must be the case.)
- Ensure you are using the wired LAN interface. The Wireless interface can only be used if its configuration matches your PC's wireless settings.

Setup Wizard

The first time you connect to the Wireless Router, the Setup Wizard must be run.

1. Step through the Wizard until finished.
   - You need to know the type of Internet connection service used by your ISP. Check the data supplied by your ISP.
   - The common connection types are explained in the tables below.
2. On the final screen of the Wizard, run the test and check that an Internet connection can be established.
3. If the connection test fails:
   - Check your data, the Cable/DSL modem, and all connections.
   - Check that you have entered all data correctly.
   - If using a Cable modem, your ISP may have recorded the MAC (physical) address of your PC. Run the Wizard, and on the *Cable Modem* screen, use the "Clone MAC address" button to copy the MAC address from your PC to the Wireless Router.

Common Connection Types

Cable Modems

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	Usually, none. However, some ISP's may require you to use a particular Hostname, Domain name, or MAC (physical) address.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you. Some ISP's may also require you to use a particular Hostname, Domain name, or MAC (physical) address.

DSL Modems

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	None.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you.
PPPoE	You connect to the ISP only when required. The IP address is usually allocated automatically.	User name and password.
PPTP	PPTP is mainly used in Europe. You connect to the ISP only when required. The IP address is usually allocated automatically, but may be Static (Fixed).	• Server IP Address. • User name and password. • IP Address allocated to you, if Static (Fixed).

Other Modems (e.g. Broadband Wireless)

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	None.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you.

Big Pond (Australia)

For this connection method, the following data is required:

- User Name
- Password
- Big Pond Server IP address

SingTel RAS

For this connection method, the following data is required:

- User Name
- Password
- RAS Plan

Home Screen

You will see the *Home* screen when you access the Wireless Broadband router. Please run **Setup Wizard** for the first time. An example screen is shown below.

Figure 5: Home Screen

Main Menu

The main menu, on the left, contains links to the most-commonly used screen.

The main menu also contains two (2) buttons:

- **Log Out** - When finished, you should click this button to logout.
- **Restart** - Use this if you wish to restart the Wireless Broadband Router. Note that restarting the Router will break any existing connections to or through the Router.

Navigation & Data Input

- Use the menu bar on the left of the screen, and the "Back" button on your Browser, for navigation.
- Changing to another screen without clicking "Save" does NOT save any changes you may have made. You must "Save" before changing screens or your data will be ignored.

On each screen, clicking the "Help" button will display help for that screen.

LAN Screen

Use the *LAN* link on the main menu to reach the LAN screen. An example screen is shown below.

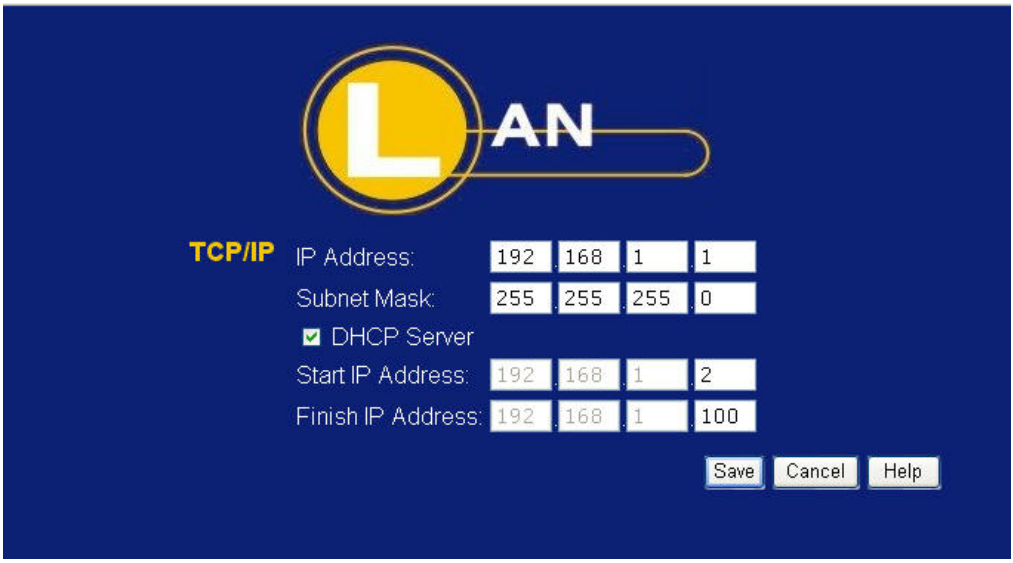

Figure 6: LAN Screen

Data - LAN Screen

TCP/IP	
IP Address	IP address for the Wireless Broadband Router, as seen from the local LAN. Use the default value unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN.
Subnet Mask	The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Subnet Mask for the LAN segment to which the Wireless Broadband Router is attached (the same value as the PCs on that LAN segment).
DHCP Server	• If Enabled, the Wireless Broadband Router will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default (and recommended) value is Enabled. • If you are already using a DHCP Server, this setting must be Disabled, and the existing DHCP server must be re-configured to treat the Wireless Broadband Router as the default Gateway. See the following section for further details. • The **Start IP Address** and **Finish IP Address** fields set the values used by the DHCP server when allocating IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported. See the following section for further details on using DHCP.

DHCP

What DHCP Does

A DHCP (Dynamic Host Configuration Protocol) **Server** allocates a valid IP address to a DHCP **Client** (PC or device) upon request.

- The client request is made when the client device starts up (boots).
- The DHCP Server provides the *Gateway* and *DNS* addresses to the client, as well as allocating an IP Address.
- The Wireless Broadband Router can act as a **DHCP server**.
- Windows and other non-Server versions of Windows will act as a DHCP **client**. This is the default Windows setting for the TCP/IP network protocol. However, Windows uses the term *Obtain an IP Address automatically* instead of "DHCP Client".
- You must NOT have two (2) or more DHCP Servers on the same LAN segment. (If you only have one Router on your LAN, then there must only be one (1) DHCP Server on your LAN.)

Using the Wireless Broadband Router's DHCP Server

This is the default setting. The DHCP Server settings are on the ***LAN*** screen. On this screen, you can:

- Enable or Disable the Wireless Broadband Router's DHCP *Server* function.
- Set the range of IP Addresses allocated to PCs by the DHCP Server function.

You can assign Fixed IP Addresses to some devices while using DHCP, provided that the Fixed IP Addresses are NOT within the range used by the DHCP Server.

Using another DHCP Server

You can only use one (1) DHCP Server per LAN segment. If you wish to use another DHCP Server, rather than the Wireless Broadband Router's, the following procedure is required.

- Disable the DHCP Server feature in the Wireless Broadband Router. This setting is on the LAN screen.
- Configure the DHCP Server to provide the Wireless Broadband Router's IP Address as the *Default Gateway*.

To Configure your PCs to use DHCP

This is the default setting for TCP/IP for all non-Server versions of Windows.

See *Chapter 4 - Client Configuration* for the procedure to check these settings.

Wireless Screen

The Wireless Broadband Router's settings must match the other Wireless stations.

Note that the Wireless Broadband Router will automatically accept 802.11b, 802.11g and 802.11n Draft, and no configuration is required for this feature.

To change the Wireless Broadband Router's default settings for the Wireless Access Point feature, use the *Wireless* link on the main menu to reach the ***Wireless*** screen. An example screen is shown below.

Figure 7: Wireless Screen

Data - Wireless Screen

Identification	
Region	Select the correct domain for your location. It is your responsibility to ensure: • That the Wireless Broadband Router is only used in domains for which is licensed. • That you select the correct domain, so that only the legal channels for that domain can be selected.

Station name	This is the same as the "Device Name" for the Wireless Broadband Router.
SSID	This is also called the "Network Name". • If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier). • To communicate, all Wireless stations should use the same SSID/ESSID.
Options	
Mode	Select the desired mode: • **Off** - Disable Wireless AP function. • **802.11b** - Only 802.11b connections are available. 802.11g Wireless Stations will only be able to use the Wireless Broadband Router if they are fully backward-compatible with the 802.11b standard. • **802.11b + g** - Both 802.11.g and 802.11b Wireless stations will be able to use the Wireless Broadband Router. • **802.11b + g + n** - 802.11g, 802.11b and 802.11n Draft Wireless stations will be able to use the Wireless Broadband Router. • **802.11 g + n** - Both 802.11.g and 802.11n Draft Wireless stations will be able to use the Wireless Broadband Router. • **802.11n** - Only 802.11n Draft Wireless stations can use the Wireless Broadband Router.
Channel No.	Select the Channel you wish to use on your Wireless LAN. • If you experience interference (shown by lost connections and/or slow data transfers) you may need to experiment with different channels. • If using multiple Access Points, adjacent Access Points should use different Channels to reduce interference.
Broadcast SSID	If enabled, the Wireless Broadband Router will broadcast its SSID. This allows PCs and other wireless stations to detect this Access Point and use the correct SSID. The default SSID is **WBR-6000** If disabled, PC users will have to manually enter the SSID and other details of the wireless interface before they can connect to this Access Point.
Wireless Security	
Current Setting	The current Wireless security is displayed. The default value is Disabled.
Configure Button	Click this button to access the Wireless security sub-screen, and view or change the settings. See the following section for details.

MAC Filter	
MAC Filter	There are 3 options: • Disabled - Select this if you don't want to use Wireless MAC Filter function. • Allow - Only the client Listed in the Station can connect to this Wireless Router .To edit the wireless stations Please click the "Set Stations". • Deny - The client listed on the stations can not use the access point, others can use this access point to access the internet or LAN.
Set Stations Button	Click this button to manage the MAC Address control stations.
Draft 802.11n Setting	
Bandwidth	Select the desired bandwidth from the drop-down list. 20MHz Only – Single Channel Bandwidth 40MHz Only – Dual-Channel Bandwidth; combine channels result with high performance. 20MHz/40MHz Auto – Auto Selection, this is the default setting. Wireless Broadband Router will auto selection depend on the bandwidth demand. Please note that selecting 20MHz Only or 40MHz Only might cause connection problem due to unmatched setting with client devices. Auto Selection is highly recommended.
Protected Mode	Select On or Off for protected mode. When Protected Mode is ON, 802.11n Draft transmission will be treated as first priority.

Wireless Security

This screen is accessed by clicking the "Configure" button on the *Wireless* screen. There are 3 options for Wireless security:

- **Disabled** - no data encryption is used.
- **WEP** - data is encrypted using the WEP standard.
- **WPA-PSK** - data is encrypted using the WPA-PSK standard. This is a later standard than WEP, and provides much better security than WEP. If all your Wireless stations support WPA-PSK, you should use WPA-PSK rather than WEP.
- **WPA2-PSK** - This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption.
- **WPA-PSK and WPA2-PSK** - This method, sometimes called "Mixed Mode", allows clients to use EITHER WPA-PSK (with TKIP) OR WPA2-PSK (with AES).

WEP Wireless Security

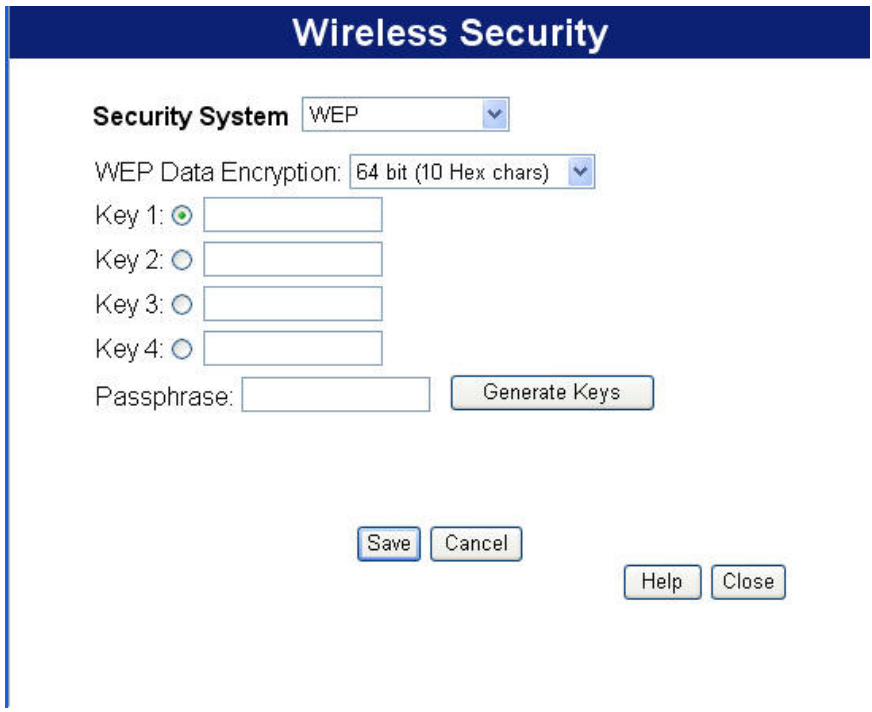

Figure 8: WEP

Data - WEP Screen

WEP Data Encryption	
WEP Data Encryption	Select the desired option, and ensure the Wireless Stations use the same setting. • **64 Bit** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is 10 chars in HEX (0~9 and A~F). • **128 Bit** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key.

	For 128 Bit Encryption, the key size is 26 chars in HEX (0~9 and A~F).
Key 1 ~ 4	Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. You must enter a **Key Value** for the **Default Key**.
Key Value	Enter the key value or values you wish to use. The **Key** is required, the other keys are optional. Other stations must have the same key.
Passphrase	If desired, you can generate a key from a phrase, instead of entering the key value directly. Enter the desired phrase, and click the "Generate Keys" button.

WPA-PSK Wireless Security

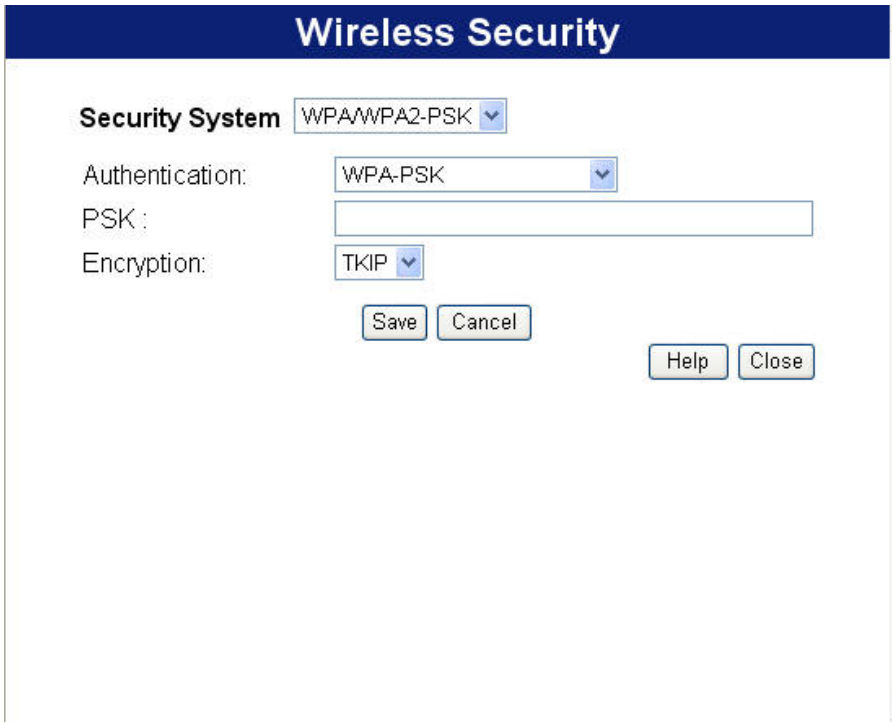

Figure 9: WPA-PSK

Data - WPA-PSK Screen

Authentication	**WPA-PSK** Like WEP, data is encrypted before transmission. WPA is more secure than WEP, and should be used if possible. WPA-PSK is the version of WPA, which does NOT require a Radius Server on your LAN.
PSK	Enter the PSK (network key). Data is encrypted using a key derived from the network key. Other Wireless Stations must use the same network key. The PSK must be from 8 to 63

	characters in length.
WPA Encryption	The WPA-PSK standard allows different encryption methods to be used. Select the desired option (TKIP or AES). Wireless Stations must use the same encryption method enable to establish connection.

WPA2-PSK Wireless Security

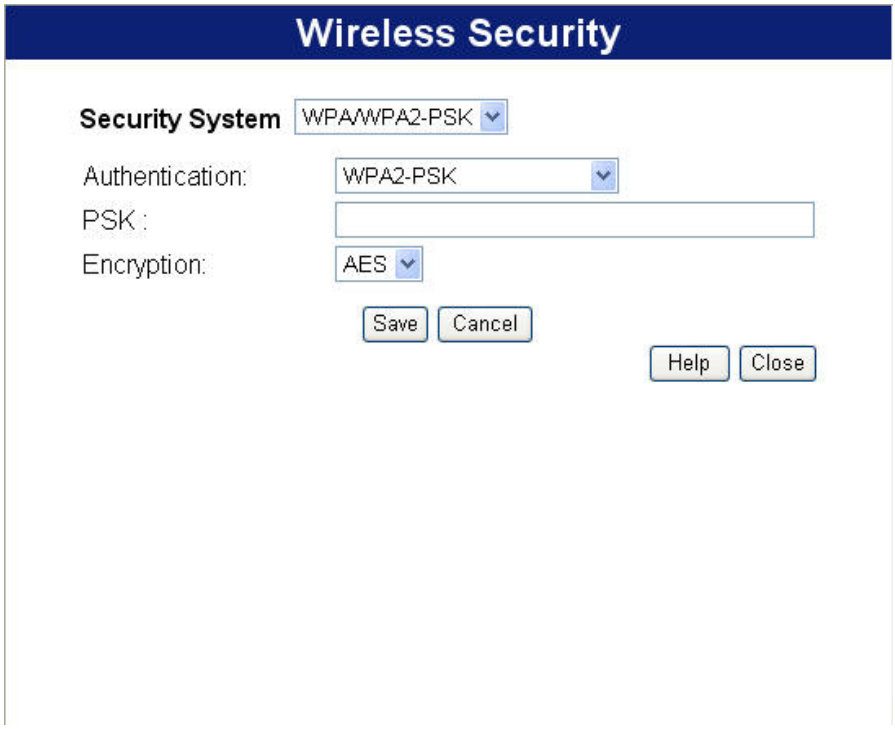

Figure 10: WPA2-PSK

Data - WPA2-PSK Screen

Authentication	**WPA2-PSK** This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption.
PSK	Enter the PSK (network key). Data is encrypted using a key derived from the network key. Other Wireless Stations must use the same network key. The PSK must be from 8 to 63 characters in length.
Encryption	The WPA2-PSK standard allows using AES encryption method only. Please note that wireless stations must use the same encryption method.

WPA-PSK+WPA2-PSK Wireless Security

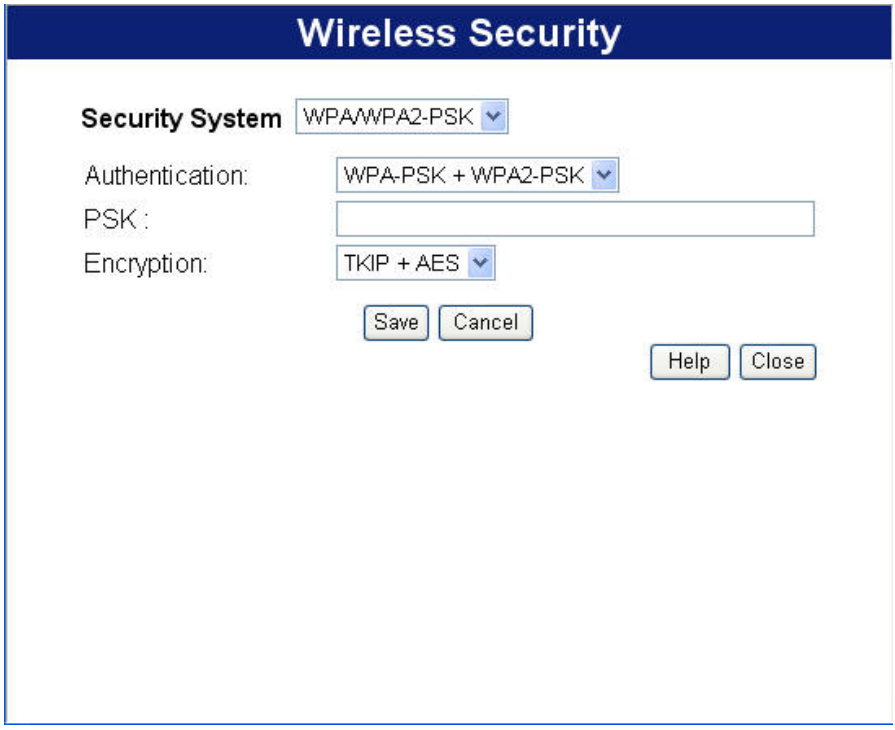

Figure 11: WPA-PSK+WPA2-PSK

Data - WPA-PSK+WPA2-PSK Screen

Authentication	**WPA-PSK+WPA2-PSK** This method, sometimes called "Mixed Mode", allows clients to use EITHER WPA-PSK (with TKIP) OR WPA2-PSK (with AES).
PSK	Enter the PSK (network key). Data is encrypted using a key derived from the network key. Other Wireless Stations must use the same network key. The PSK must be from 8 to 63 characters in length.
Encryption	The WPA/WPA2-PSK standard allows different encryption methods to be used in the same time. Wireless Stations must use the same encryption method.

Password Screen

The password screen allows you to assign a password to the Wireless Broadband Router.

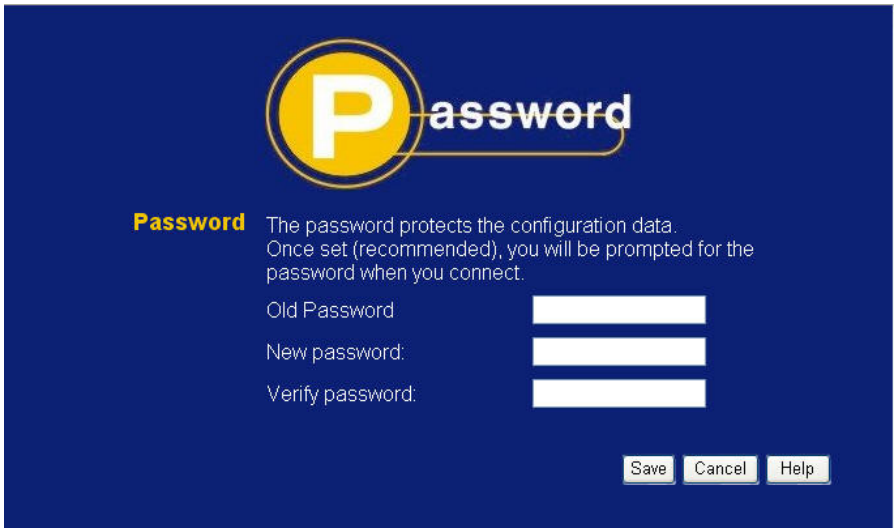

Figure 12: Password Screen

Old Password	Enter the existing password in this field.
New password	Enter the new password here.
Verify password	Re-enter the new password here.

You will be prompted for the password when you connect, as shown below.

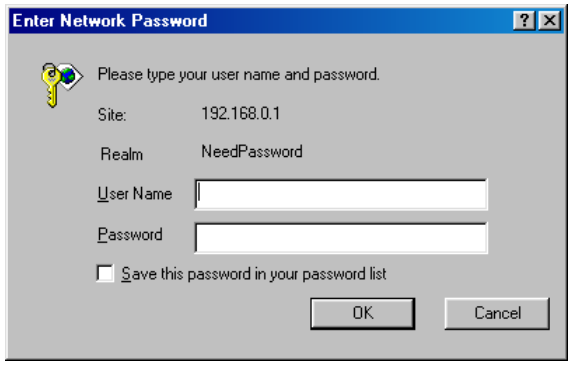

Figure 13: Password Dialog

- The "User Name" is always admin
- Enter the password for the Wireless Broadband Router, as set on the *Password* screen above. The default password is **password**.

Chapter 4
PC Configuration

This Chapter details the PC Configuration required on the local ("Internal") LAN.

Overview

For each PC, the following may need to be configured:

- TCP/IP network settings
- Internet Access configuration
- Wireless configuration

Windows Clients

This section describes how to configure Windows clients for Internet access via the Wireless Broadband Router.

The first step is to check the PC's TCP/IP settings.

The Wireless Broadband Router uses the TCP/IP network protocol for all functions, so it is essential that the TCP/IP protocol be installed and configured on each PC.

TCP/IP Settings - Overview

If using the default Wireless Broadband Router settings, and the default Windows TCP/IP settings, no changes need to be made.

- By default, the Wireless Broadband Router will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

If using a Fixed (specified) IP address, the following changes are required:

- The *Gateway* must be set to the IP address of the Wireless Broadband Router
- The *DNS* should be set to the address provided by your ISP.

If your LAN has a Router, the LAN Administrator must reconfigure the Router itself. Refer to *Chapter 8 - Advanced Setup* for details.

Checking TCP/IP Settings - Windows 9x/ME:

1. Select *Control Panel - Network*. You should see a screen like the following:

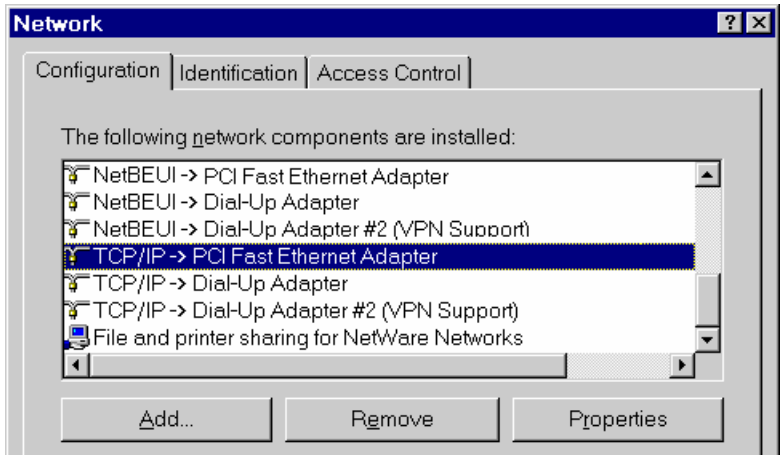

Figure 14: Network Configuration

2. Select the *TCP/IP* protocol for your network card.
3. Click on the *Properties* button. You should then see a screen like the following.

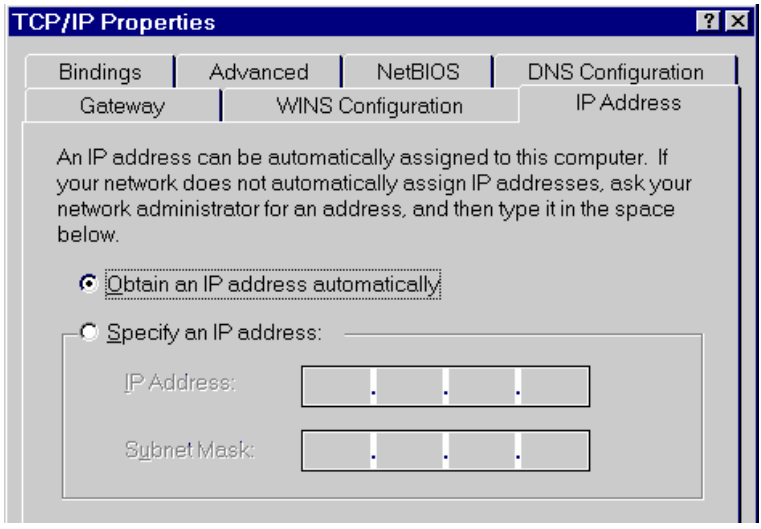
TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:

Figure 15: IP Address (Win 9x)

Ensure your TCP/IP settings are correct, as follows:

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended**. By default, the Wireless Broadband Router will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the Wireless Broadband Router.

Using "Specify an IP Address"

If your PC is already configured, check with your network administrator before making the following changes:

- On the *Gateway* tab, enter the Wireless Broadband Router's IP address in the *New Gateway* field and click *Add*, as shown below. Your LAN administrator can advise you of the IP Address they assigned to the Wireless Broadband Router.

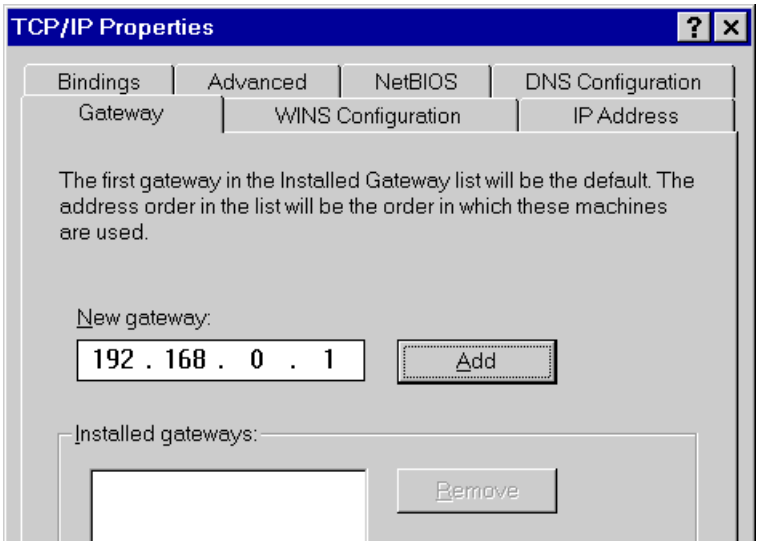

Figure 16: Gateway Tab (Win 9x)

- On the *DNS Configuration* tab, ensure *Enable DNS* is selected. If the *DNS Server Search Order* list is empty, enter the DNS address provided by your ISP in the fields beside the *Add* button, then click *Add*.

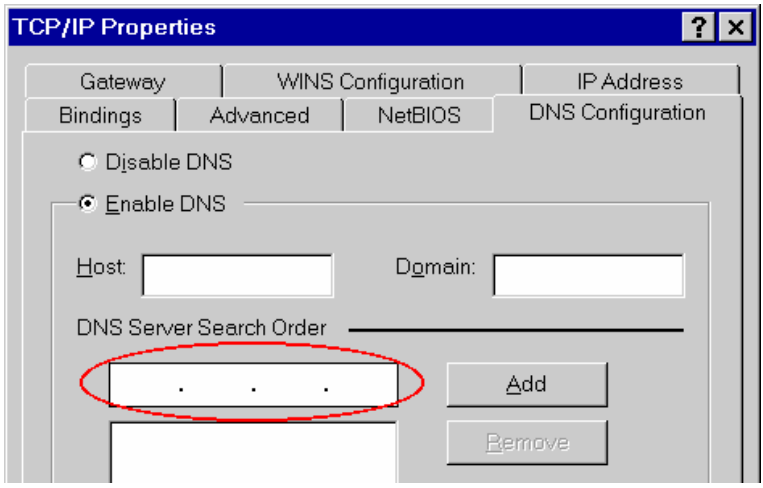

Figure 17: DNS Tab (Win 9x)

Checking TCP/IP Settings - Windows 2000:

1. Select *Control Panel - Network and Dial-up Connection*.
2. Right - click the *Local Area Connection* icon and select *Properties*. You should see a screen like the following:

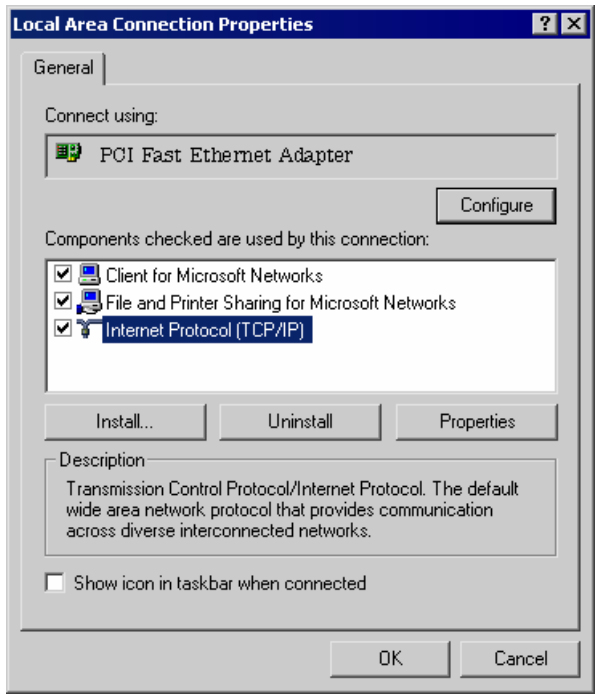

Figure 18: Network Configuration (Win 2000)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

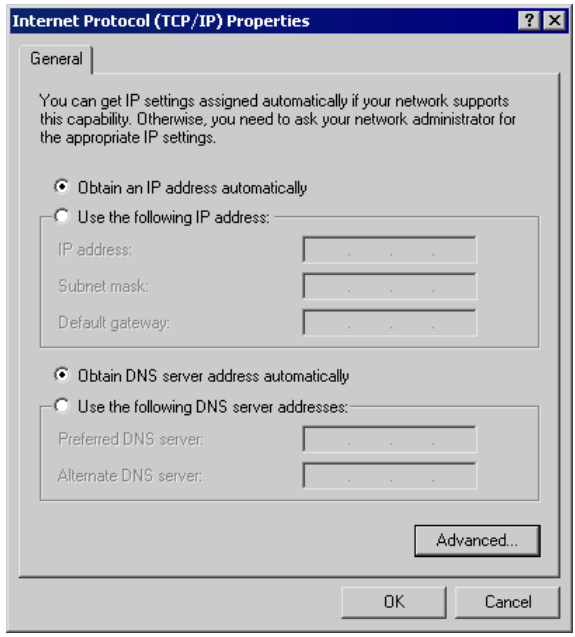
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 19: TCP/IP Properties (Win 2000)

5. Ensure your TCP/IP settings are correct, as described below.

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended**. By default, the Wireless Broadband Router will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the Wireless Broadband Router.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- Enter the Wireless Broadband Router's IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to the Wireless Broadband Router.)
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

Checking TCP/IP Settings - Windows XP

1. Select *Control Panel - Network Connection*.
2. Right click the *Local Area Connection* and choose *Properties*. You should see a screen like the following:

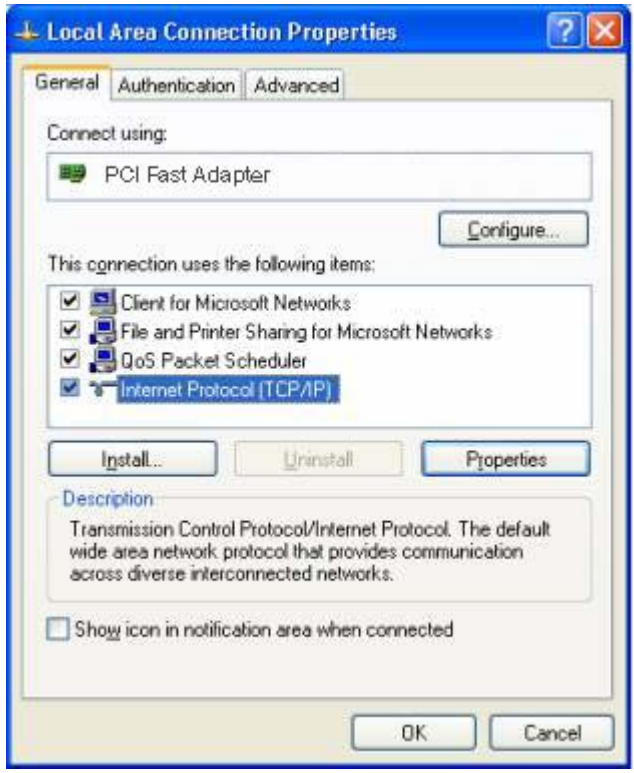

Figure 20: Network Configuration (Windows XP)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

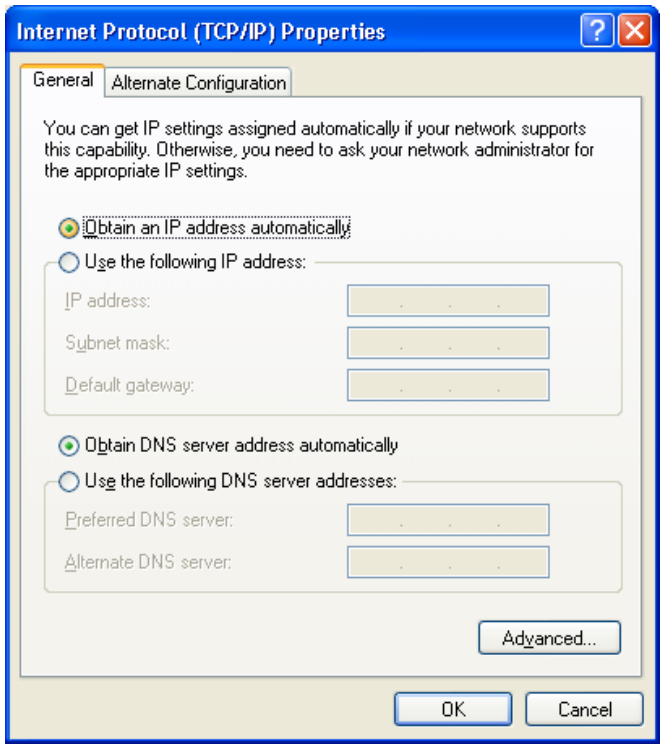
Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 21: TCP/IP Properties (Windows XP)

5. Ensure your TCP/IP settings are correct.

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended**. By default, the Wireless Broadband Router will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the Wireless Broadband Router.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- In the *Default gateway* field, enter the Wireless Broadband Router's IP address and click *OK*. Your LAN administrator can advise you of the IP Address they assigned to the Wireless Broadband Router.
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

Internet Access

To configure your PCs to use the Wireless Broadband Router for Internet access:

- Ensure that the DSL modem, Cable modem, or other permanent connection is functional.
- Use the following procedure to configure your Browser to access the Internet via the LAN, rather than by a Dial-up connection.

For Windows 9x/ME/2000

1. Select *Start Menu - Settings - Control Panel - Internet Options*.
2. Select the Connection tab, and click the *Setup* button.
3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click *Next*.
4. Select "I connect through a local area network (LAN)" and click *Next*.
5. Ensure all of the boxes on the following Local area network Internet Configuration screen are **unchecked**.
6. Check the "No" option when prompted "Do you want to set up an Internet mail account now?"
7. Click *Finish* to close the Internet Connection Wizard.
   Setup is now completed.

For Windows XP

1. Select *Start Menu - Control Panel - Network and Internet Connections*.
2. Select *Set up or change your Internet Connection*.
3. Select the *Connection* tab, and click the *Setup* button.
4. Cancel the pop-up "Location Information" screen.
5. Click *Next* on the "New Connection Wizard" screen.
6. Select "Connect to the Internet" and click *Next*.
7. Select "Set up my connection manually" and click *Next*.
8. Check "Connect using a broadband connection that is always on" and click *Next*.
9. Click *Finish* to close the New Connection Wizard.
   Setup is now completed.

Accessing AOL

To access AOL (America On Line) through the Wireless Broadband Router, the *AOL for Windows* software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

- Start the *AOL for Windows* communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
- Click the *Setup* button.
- Select *Create Location*, and change the location name from "New Locality" to "Wireless Broadband Router".
- Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* blank.)
- Click *Save*, then *OK*.
  Configuration is now complete.
- Before clicking "Sign On", always ensure that you are using the "Wireless Broadband Router" location.

Macintosh Clients

From your Macintosh, you can access the Internet via the Wireless Broadband Router. The procedure is as follows.

1. Open the TCP/IP Control Panel.
2. Select *Ethernet* from the *Connect via* pop-up menu.
3. Select *Using DHCP Server* from the *Configure* pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

Note:

If using manually assigned IP addresses instead of DHCP, the required changes are:

- Set the *Router Address* field to the Wireless Broadband Router's IP Address.
- Ensure your DNS settings are correct.

Linux Clients

To access the Internet via the Wireless Broadband Router, it is only necessary to set the Wireless Broadband Router as the "Gateway".

Ensure you are logged in as "root" before attempting any changes.

Fixed IP Address

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

- Set your "Default Gateway" to the IP Address of the Wireless Broadband Router.
- Ensure your DNS (Name server) settings are correct.

To act as a DHCP Client (recommended)

The procedure below may vary according to your version of Linux and X -windows shell.

1. Start your X Windows client.
2. Select *Control Panel - Network*
3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
4. Click the *Edit* button, set the "protocol" to "DHCP", and save this data.
5. To apply your changes
    - Use the "Deactivate" and "Activate" buttons, if available.
    - OR, restart your system.

Other Unix Systems

To access the Internet via the Wireless Broadband Router:

- Ensure the "Gateway" field for your network card is set to the IP Address of the Wireless Broadband Router.
- Ensure your DNS (Name Server) settings are correct.

Wireless Station Configuration

This section applies to all Wireless stations wishing to use the Wireless Broadband Router's Access Point, regardless of the operating system which is used on the client.

To use the Wireless Access Point in the Wireless Broadband Router, each Wireless Station must have compatible settings, as follows:

Mode	The mode must be set to ***Infrastructure*** (rather than Ad-hoc) Access points only operate in ***Infrastructure*** mode.
SSID (ESSID)	This must match the value used on the Wireless Broadband Router. The default value is **WBR-6000**.
Wireless Security	By default, Wireless security on the Wireless Broadband Router is disabled. • If Wireless security remains disabled on the Wireless Broadband Router, all stations must have wireless security disabled. • If Wireless security is enabled on the Wireless Router (either WEP or WPA-PSK), each station must use the same settings as the Wireless Broadband Router.

Chapter 5
Operation and Status

This Chapter details the operation of the Wireless Broadband Router and the status screens.

Operation

Once both the Wireless Broadband Router and the PCs are configured, operation is automatic.

However, there are some situations where additional Internet configuration may be required. Refer to *Chapter 6 - Advanced Features* for further details.

Status Screen

Use the ***Status*** link on the main menu to view this screen.

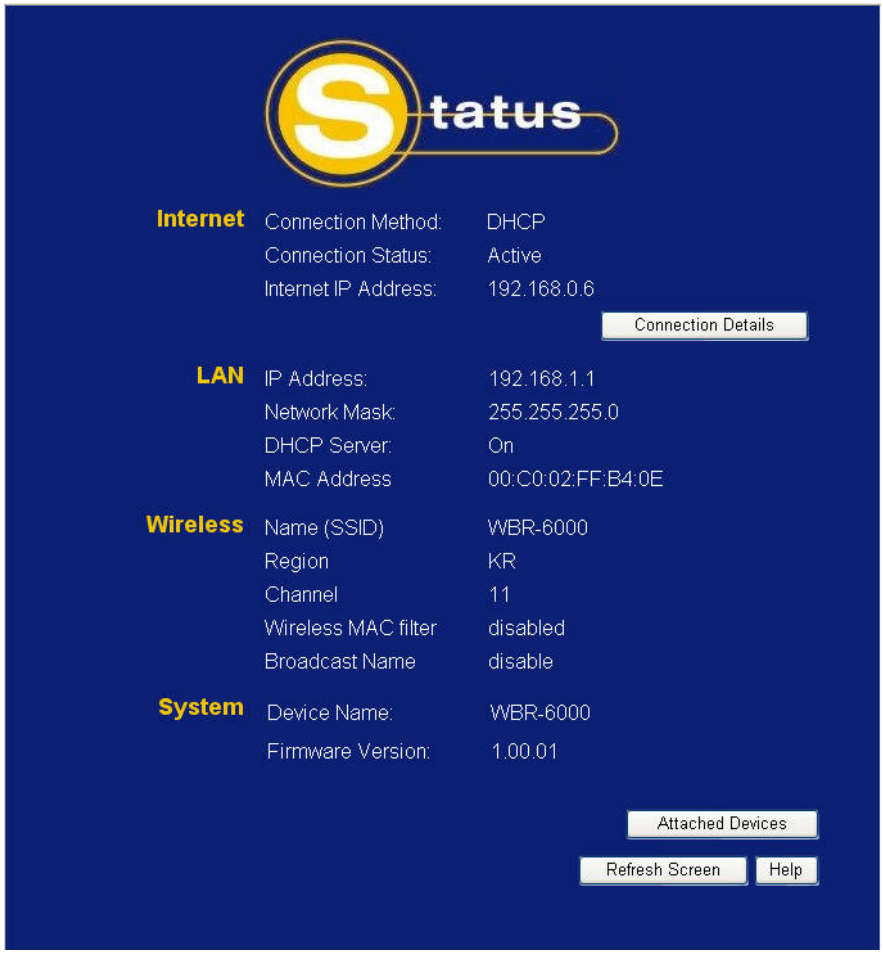

Figure 22: Status Screen

Data - Status Screen

Internet	
Connection Method	Displays the current connection method, as set in the *Setup Wizard*.
Connection Status	This indicates the current status of the Internet Connection • **Active** - Connection exists • **Idle** - No current connection, but no error has been detected. This condition normally arises when an idle connection is automatically terminated. • **Failed** - The connection was terminated abnormally. This could be caused by Modem failure or the loss of the connection to the ISP's server. If there is an error, you can click the "Connection Details" button to find out more information.
Internet IP Address	This IP Address is allocated by the ISP (Internet Service Provider). If using a dynamic IP address and no connection currently exists, this information is unavailable.
Connection Details	Click this button to open a sub-window and view a detailed description of the current connection. Depending on the type of connection, a "log" may also be available.
LAN	
IP Address	The IP Address of the Wireless Broadband Router.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
DHCP Server	This shows the status of the DHCP Server function. The value will be "Enabled" or "Disabled".
MAC Address	This shows the MAC Address for the Wireless Broadband Router, as seen on the LAN interface.
Wireless	
Name (SSID)	If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier).
Region	The current region, as set on the Wireless screen.
Channel	This shows the Channel currently used, as set on the Wireless screen.
Wireless AP	This indicates whether or not the Wireless Access Point feature is enabled.
Broadcast Name	This indicates whether or not the SSID is Broadcast. This setting is on the Wireless screen.
System	
Device Name	The current name of the Router.
Firmware Version	The version of the current firmware installed.

Buttons	
Connection Details	Click this button to open a sub-window and view a detailed description of the current connection.
Attached Devices	This will open a sub-window, showing all LAN and Wireless devices currently on the network.
Refresh Screen	Update the data displayed on screen.

Connection Status - PPPoE

If using PPPoE (PPP over Ethernet) a screen like the following example will be displayed when the "Connection Details" button is clicked.

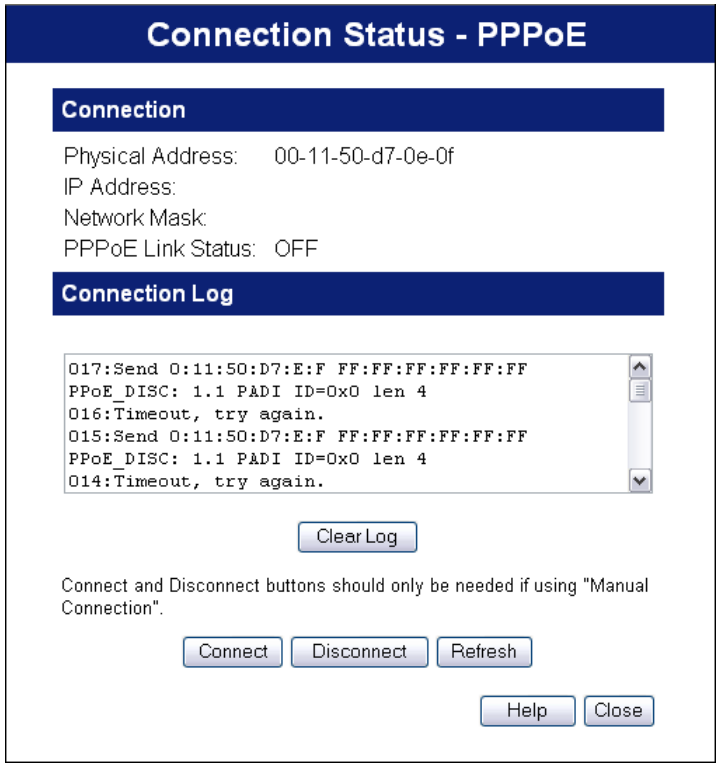

Figure 23: PPPoE Status Screen

Data - PPPoE Screen

Connection Time	This indicates how long the current connection has been established.
Connection to Server	This indicates whether or not the connection is currently established.
Negotiation	This indicates the status of the PPPoE Server login.
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Close	Close this window.

Connection Status - PPTP

If using PPTP (Peer-to-Peer Tunneling Protocol), a screen like the following example will be displayed when the "Connection Details" button is clicked.

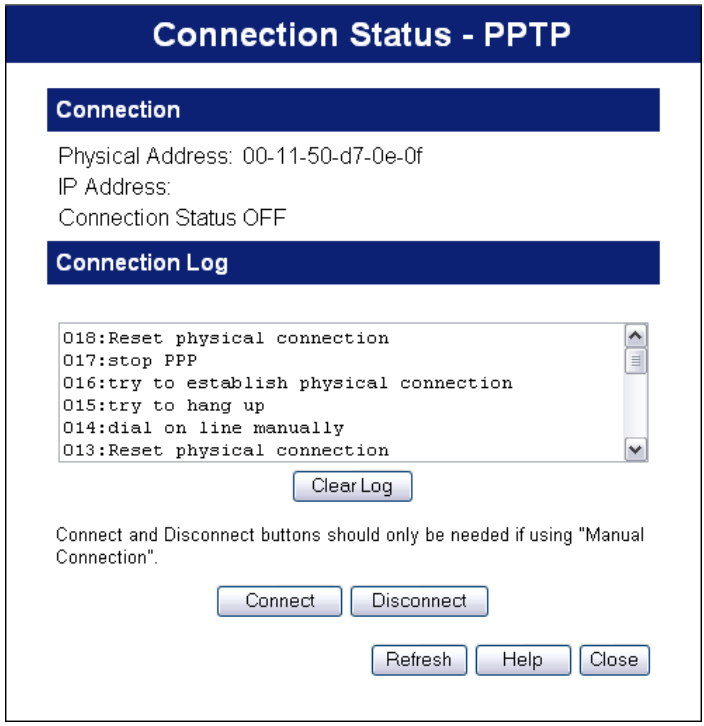

Figure 24: PPTP Status Screen

Data - PPTP Screen

Connection	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Connection Status	• This indicates whether or not the connection is currently established. • If the connection does not exist, the *Connect* button can be used to establish a connection. • If the connection currently exists, the *Disconnect* button can be used to break the connection. • Normally, it is not necessary to use the *Connect* and *Disconnect* buttons unless the setting "Connect automatically, as required" is disabled.

Connection Log	
Connection Log	• The Connection Log shows status messages relating to the existing connection. • The "Clear Log" button will restart the Log, while the Refresh button will update the messages shown on screen.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, terminate the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

Connection Status - L2TP

If using L2TP, a screen like the following example will be displayed when the "Connection Details" button is clicked.

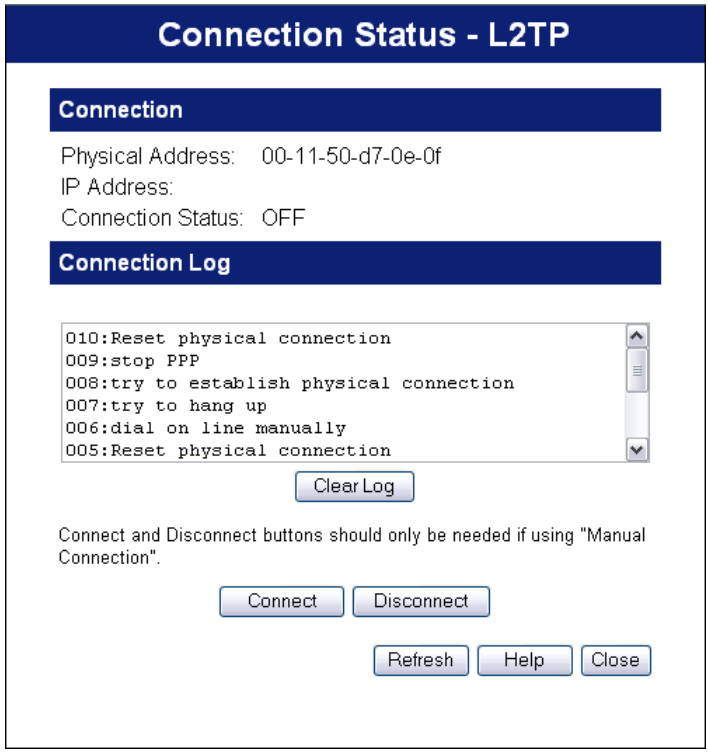

Figure 25: L2TP Status Screen

Data - L2TP Screen

Internet	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)

IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Connection Status	This indicates whether or not the connection is currently established. • If the connection does not exist, the *Connect* button can be used to establish a connection. • If the connection currently exists, the *Disconnect* button can be used to break the connection. • Normally, it is not necessary to use the *Connect* and *Disconnect* buttons unless the setting "Connect automatically, as required" is disabled.
Connection Log	
Connection Log	• The Connection Log shows status messages relating to the existing connection. • The "Clear Log" button will restart the Log, while the Refresh button will update the messages shown on screen.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

Connection Status - Telstra Big Pond

An example screen is shown below.

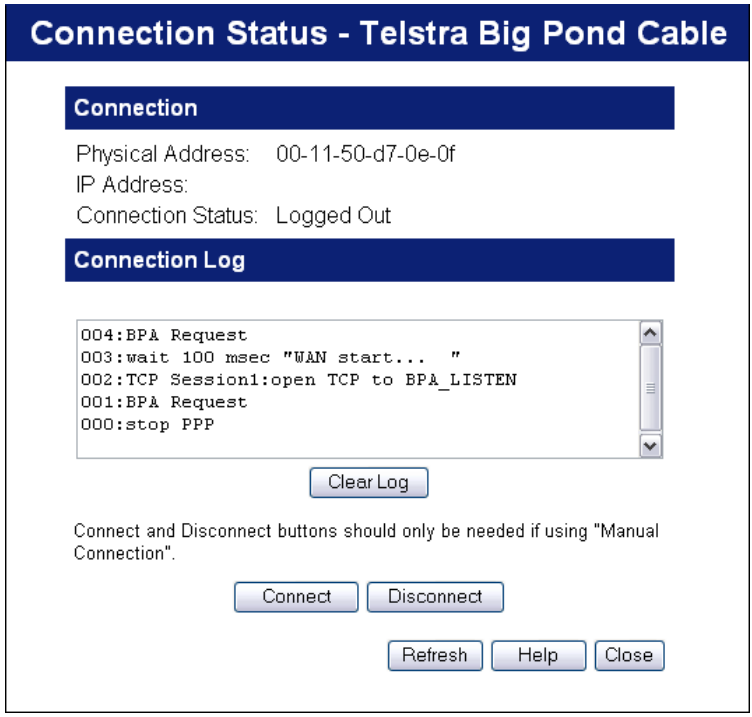

Figure 26: Telstra Big Pond Status Screen

Data - Big Pond Screen

Connection	
Physical Address	The hardware address of this device, as seen by remote devices. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Connection Status	This indicates whether or not the connection is currently established. • If the connection does not exist, the "Connect" button can be used to establish a connection. • If the connection currently exists, the "Disconnect" button can be used to break the connection. • Normally, it is not necessary to use the Connect and Disconnect buttons unless the setting "Connect automatically, as required" is disabled.
Connection Log	
Connection Log	• The Connection Log shows status messages relating to the existing connection.

	• The Clear Log button will restart the Log, while the Refresh button will update the messages shown on screen.
Buttons	
Connect	If not connected, establish a connection to Telstra Big Pond.
Disconnect	If connected to Telstra Big Pond, terminate the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

Connection Details - SingTel RAS

If using the SingTel RAS access method, a screen like the following example will be displayed when the "Connection Details" button is clicked.

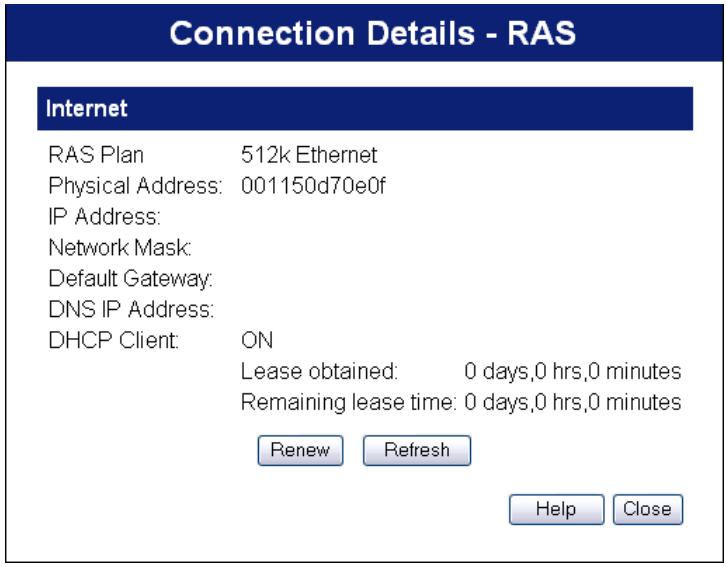

Figure 27: Connection Details - RAS

Data - RAS Screen

Internet	
RAS Plan	The RAS plan (connection speed) currently used.
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
Default Gateway	The IP Address of the remote Gateway or Broadband router associated with the IP Address above.
DNS IP Address	The IP Address of the Domain Name Server which is currently

	used.
DHCP Client	• This will show "Enabled" or "Disabled". • If "Enabled", the Internet IP Address from your ISP is allocated automatically upon connection. (Dynamic IP Address). In this case the "Lease obtained" and "Remaining lease time" fields provide additional information. Note that the lease is automatically renewed on expiry; use the "Renew" button if you wish to manually renew the lease immediately. • If "Disabled", the Internet IP Address from your ISP is Fixed or Static. In this case, the "Release/Renew" button is not operational.
Buttons	
Release/Renew	This button is only useful if the IP address shown above is allocated automatically on connection. (Dynamic IP address). Otherwise, it has no effect. • This button will say "Release" if the Wireless Broadband router is currently using an IP Address allocated by the ISP's DHCP Server. Clicking the "Release" button will release the IP Address and break the connection. • If the button says "Renew", this indicates that the ISP's DHCP Server has not allocated an IP Address for the Wireless Broadband router. Clicking the "Renew" button will re-establish the connection and obtain an IP Address from the ISP's DHCP Server.
Refresh	Update the data shown on screen.

Connection Details - Dynamic IP Address

If your access method is "Direct" (no login), with a Dynamic IP address, a screen like the following example will be displayed when the "Connection Details" button is clicked.

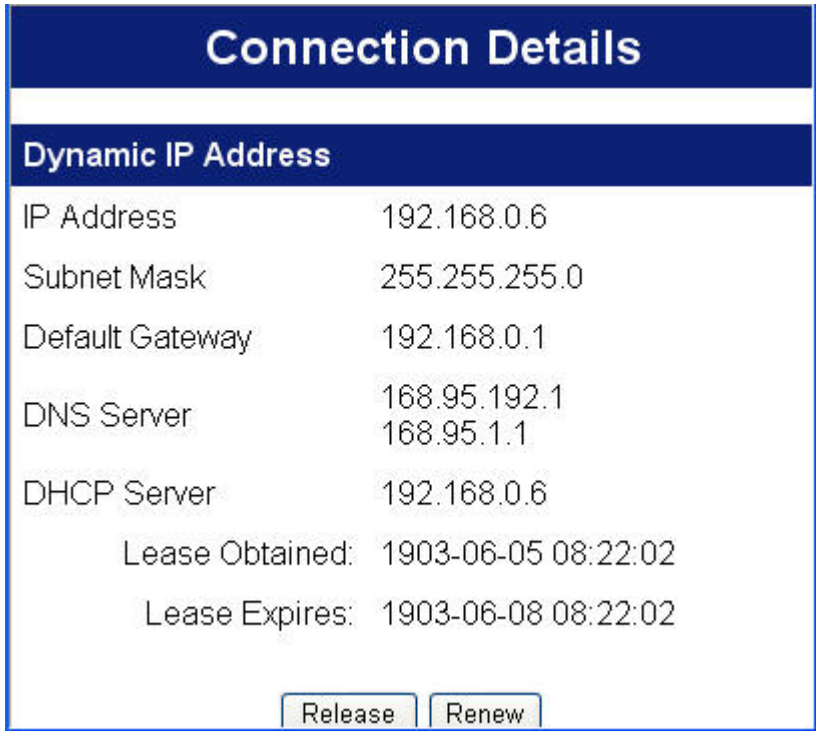

Figure 28: Connection Details - Fixed/Dynamic IP Address

Data - Dynamic IP address

Internet	
IP Address	The current IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Subnet Mask	The Subnet Mask associated with the IP Address above.
Default Gateway	The IP address of the remote Gateway or Router associated with the IP Address above.
DHCP Server	The IP address of your ISP's DHCP Server.
DNS Server	The IP address of the Domain Name Server which is currently used.
Lease Obtained **Lease Expires**	This indicates when the current IP address was obtained, and how long before this IP address allocation (the DCHP lease) expires.
Buttons	
Release	If an IP Address has been allocated to the Wireless Broadband Router (by the ISP's DHCP Server, clicking the "Release" button will break the connection and release the IP Address.

Renew	If the ISP's DHCP Server has NOT allocated an IP Address for the Wireless Broadband Router, clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server.
Close	Close this window.

Connection Details - Fixed IP Address

If your access method is "Direct" (no login), with a fixed IP address, a screen like the following example will be displayed when the "Connection Details" button is clicked.

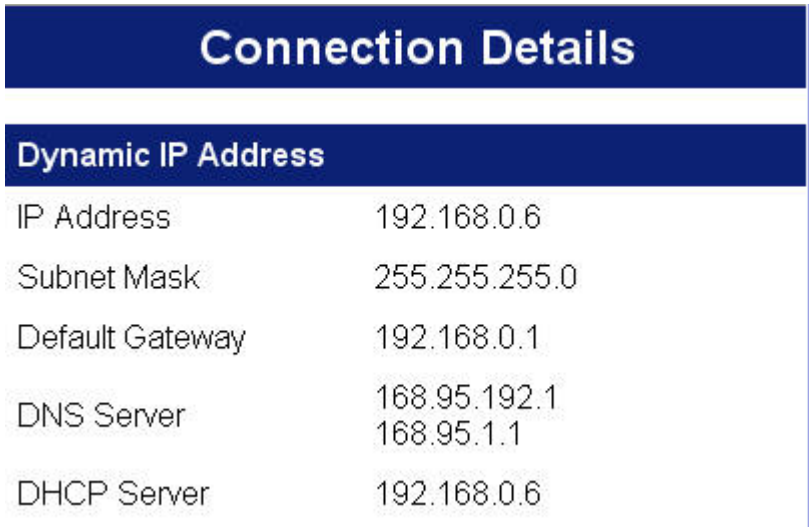

Figure 29: Connection Details - Fixed/Dynamic IP Address

Data - Fixed IP address Screen

Internet	
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Subnet Mask	The Subnet Mask associated with the IP Address above.
Default Gateway	The IP Address of the remote Gateway or Router associated with the IP Address above.
DNS Server	The IP Address of the Domain Name Server which is currently used.

Chapter 6
Advanced Features

This Chapter explains when and how to use the Wireless Broadband Router's "Advanced" Features.

Overview

The following advanced features are provided:

- Internet:
  - DMZ
  - URL filter
- Access Control
- Dynamic DNS
- Firewall Rules
- Firewall Services
- Virtual Servers
- Options
- Schedule

Internet

This screen provides access to the DMZ, Special Applications and URL Filter features.

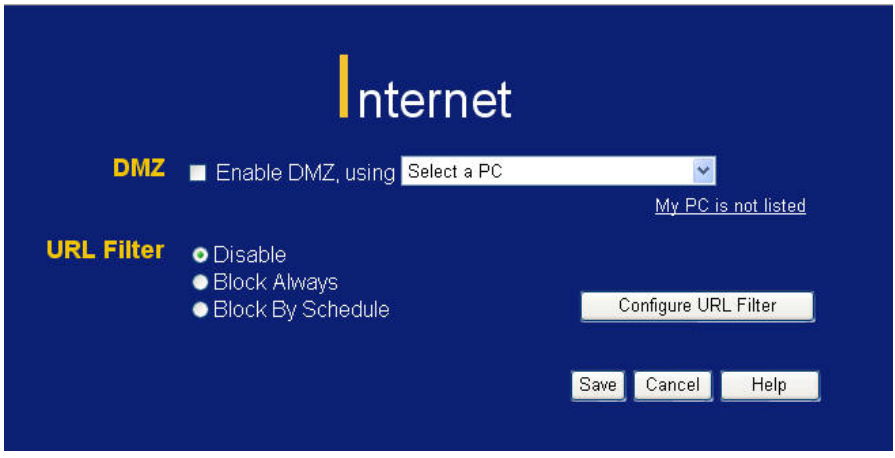

Figure 30: Internet Screen

DMZ

This feature, if enabled, allows the DMZ computer on your LAN to be exposed to all users on the Internet.

- This allows almost any application to be used on the "DMZ PC".
- The "DMZ PC" will receive all "Unknown" connections and data.

- If the DMZ feature is enabled, you must select the PC to be used as the "DMZ PC".

The "DMZ PC" is effectively outside the Firewall, making it more vulnerable to attacks. For this reason, you should only enable the DMZ feature when required.

URL Filter

If you want to limit access to certain sites on the Internet, you can use this feature. The URL filter will check each Web site access. If the address, or part of the address, is included in the block site list, access will be denied.

On the *Advanced Internet* screen, select the desired setting:

- **Disable** - disable this feature.
- **Block Always** - allow blocking all of the time, independent of the *Schedule* page.
- **Block By Schedule** - block according to the settings on the *Schedule* page.

Click the **Configure URL Filter** button to open the URL Filter screen, allowing you to create or modify the filter strings which determine which sites will be blocked.

The ***URL Filter*** screen is displayed when the **Configure URL Filter** button on the *Advanced Internet* screen is clicked.

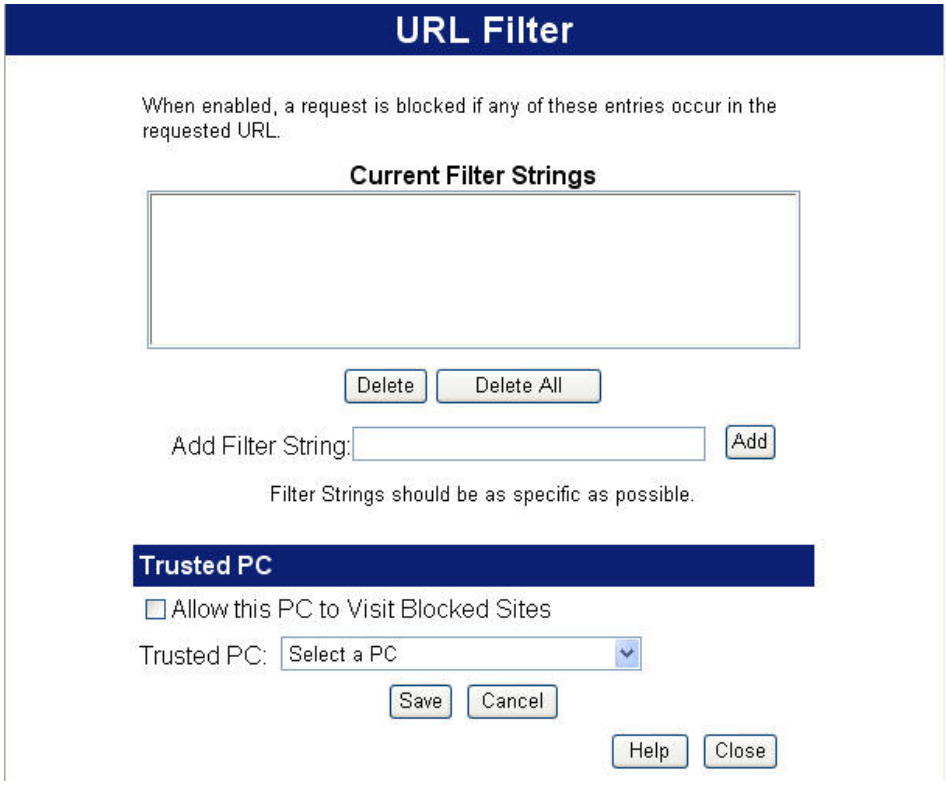

Figure 31: URL Filter Screen

Data - URL Filter Screen

Current Filter Strings	
Current Filter Strings	The list contains the current list of items to block. • To add to the list, use the "Add" option below. • To delete an entry, select it and click **Delete** button. • To delete all entries, click the **Delete All** button.
Add Filter String	To add to the current list, type the word or domain name you want to block into the field provided, then click the **Add** button. Filter strings should be as specific as possible. Otherwise, you may block access to many more sites than intended.
Trusted PC	
Allow Trusted PC	Enable this to allow one computer to have unrestricted access to the Internet. For this PC, the URL filter will be ignored. If enabled, you must select the PC to be the trusted PC.
Trusted PC	Select the PC to be the Trusted PC.

Access Control

This feature is accessed by the *Access Control* link on the Advanced menu.

Overview

The Access Control feature allows administrators to restrict the level of Internet Access available to PCs on your LAN. With the default settings, everyone has unrestricted Internet access.

Restrictions are imposed by blocking "Services", or types of connections. All common Services are pre-defined.
If required, you can also define your own Services.

Access Control Screen

To view this screen, select the *Access Control* link on the Advanced menu.

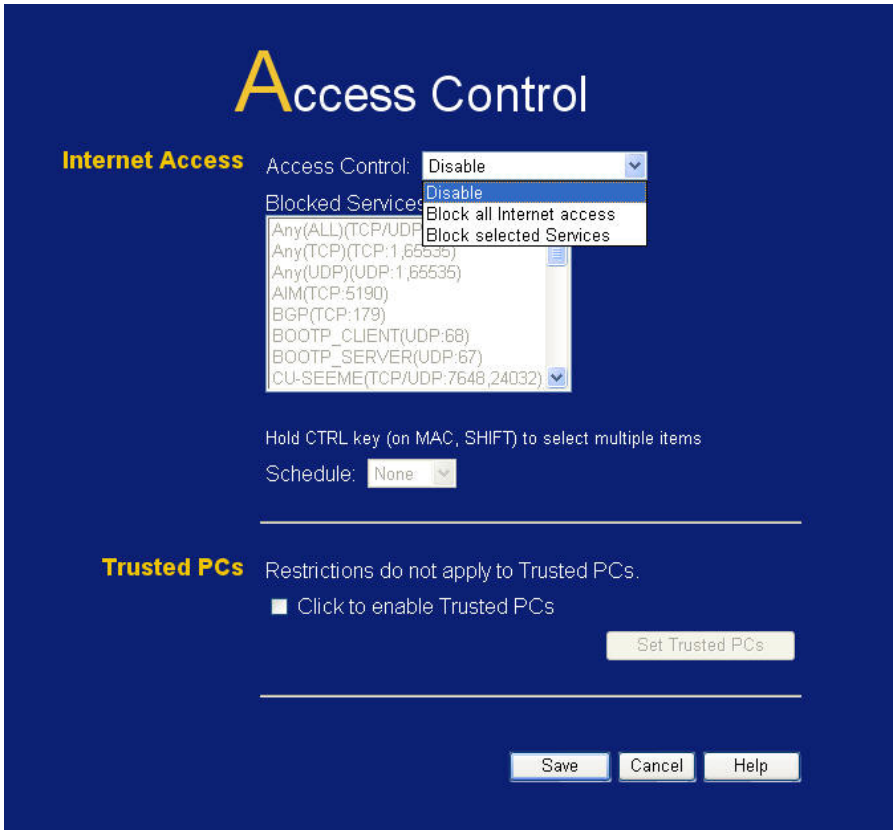

Figure 32: Access Control Screen

Data - Access Control Screen

Internet Access	
Restrictions	Select the desired options for the current group: • **None** - Nothing is blocked. Use this to create the least restrictive group. • **Block all Internet access** - All traffic via the WAN port is blocked. Use this to create the most restrictive group. • **Block selected Services** - You can select which Services are to block. Use this to gain fine control over the Internet access for a group.
Block by Schedule	If Internet access is being blocked, you can choose to apply the blocking only during scheduled times. (If access is not blocked, no Scheduling is possible, and this setting has no effect.)
Trusted PCs	
Enable Trusted PCs	Enable the checkbox if you want to use this feature.
Set Trusted PCs	Click this button to add or remove PCs from the current Group. See the following section for details of the *Trusted PCs* screen.
Buttons	
Save	Save the data on screen.
Cancel	Reverse any changes made since the last "Save".
Refresh	Update the data on screen.

Trusted PCs Screen

This screen is displayed when the *Set Trusted PCs* button on the *Access Control* screen is clicked.

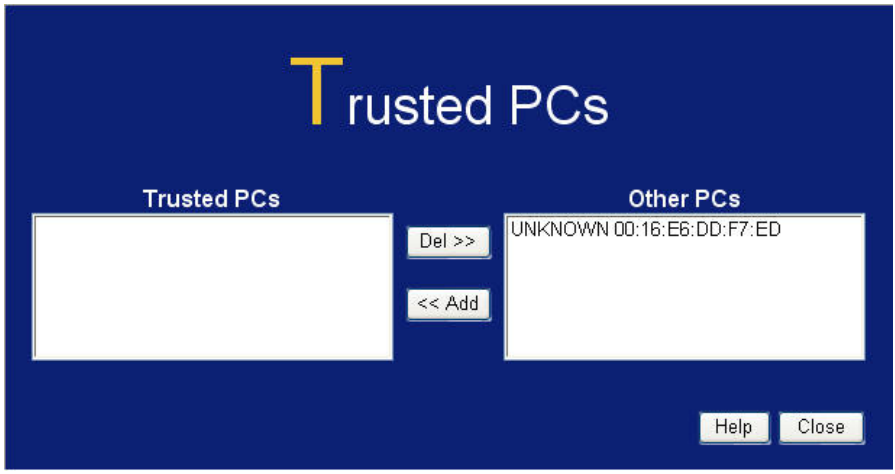

Figure 33: Trusted PCs

Use this screen to add or remove members (PCs) from the current group.

- The "Del >>" button will remove the selected PC (in the *Trusted PCs* list) from the current group.
- The "<< Add" button will add the selected PC (in the *Other PCs* list) to the current group.

Dynamic DNS (Domain Name Server)

This free service is very useful when combined with the *Virtual Server* feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address.

This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect, which makes it difficult to connect to you.

DDNS Services work as follows:

1. You must register for the service at one of the listed DDNS Service providers.
2. After registration, use the Service provider's normal procedure to obtain your desired Domain name.
3. Enter your DDNS data on the Wireless Broadband Router's DDNS screen, and enable the DDNS feature.
4. The Wireless Broadband Router will then automatically ensure that your current IP Address is recorded at the DDNS service provider's Domain Name Server.
5. From the Internet, users will be able to connect to your Virtual Servers (or DMZ PC) using your Domain name, as shown on this screen.

Dynamic DNS Screen

Select *Advanced* on the main menu, then *Dynamic DNS*, to see a screen like the following:

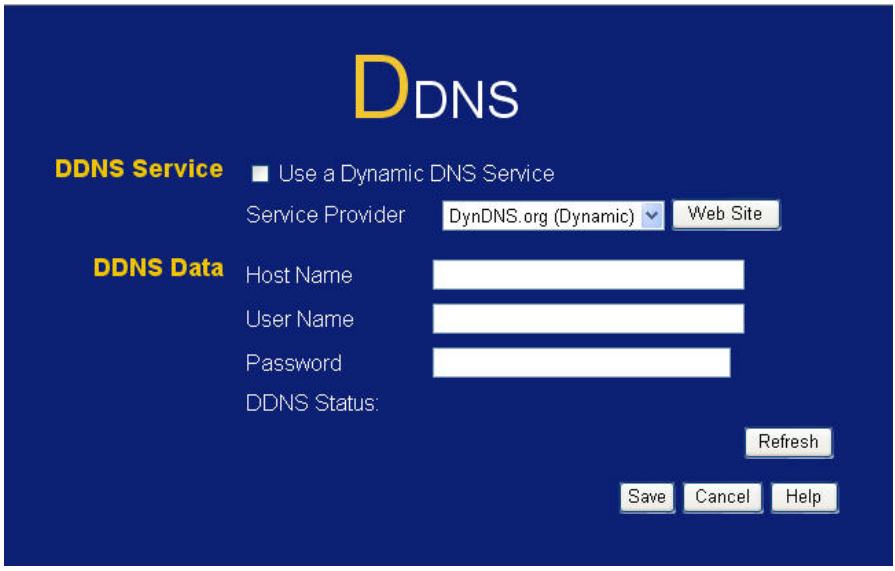

Figure 34: DDNS Screen

Data - Dynamic DNS Screen

DDNS Service	
Use a Dynamic DNS Service	Use this to enable or disable the DDNS feature as required.
Service Provider	Select the desired DDNS Service provider.

Web Site	Click this button to open a new window and connect to the Web site of the selected DDNS service provider.
DDNS Data	
Host Name	Enter the domain name allocated to you by the DDNS Service. If you have more than one name, enter the name you wish to use.
User Name	Enter your Username for the DDNS Service. (TZO.com uses your E-mail address.)
Password	Enter your current password for the DDNS Service. (TZO.com calls this a key.)
DDNS Status	• This message is returned by the DDNS Server. • Normally, this message should be "Update successful" • If the message indicates some problem, you need to connect to the DDNS Service provider and correct this problem.

Firewall Rules

The ***Firewall Rules*** screen allows you to define "Firewall Rules" which can allow or prevent certain traffic. "Traffic" means incoming connection attempts, not packets.

By default:

- All Outgoing traffic is permitted.
- All Incoming traffic is denied.

Because of this default behavior, any **Outgoing** rules will generally **Block** traffic, and **Incoming** rules will generally **Allow** traffic.

Firewall Rules Screen

An example screen is shown below.

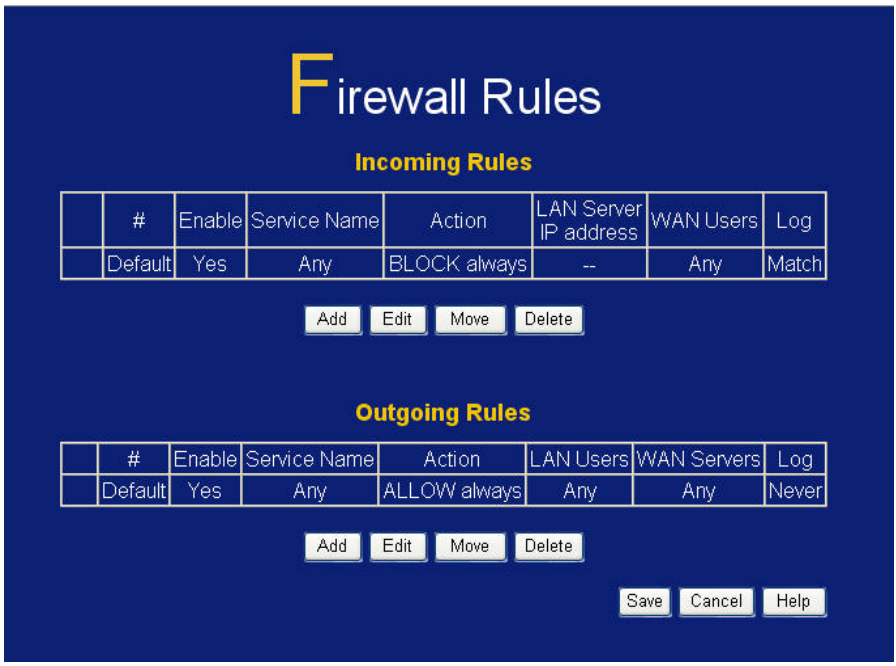
Firewall Rules
Incoming Rules
Enable Service Name Action LAN Server IP address WAN Users Log
Default Yes Any BLOCK always -- Any Match
Add Edit Move Delete
Outgoing Rules
Enable Service Name Action LAN Users WAN Servers Log
Default Yes Any ALLOW always Any Any Never
Add Edit Move Delete
Save Cancel Help

Figure 35 Firewall Screen

Data - Firewall Rules

Incoming Rules	
#	For the default rule, this will display "Default". For rules which you create, this will display a radio button which allows you to select the rule.
Enable	Indicates whether or not the rule is currently enabled. For rules you have added, this column will contain a checkbox, allowing you to easily enable or disable the rule. (Click "Save" after making any changes.)
Service Name	The Service covered by this rule.
Action	The action performed on connections which are covered by this rule.

LAN Server IP Address	The PC or Server on your LAN to which traffic covered by this rule will be sent.
WAN Users	The WAN IP address or addresses covered by this rule.
Log	Indicates whether or not connections covered by this rule should be logged.
Buttons	Use the *Add* button to create a new rule. The other buttons - *Edit*, *Move*, or *Delete* - require that a rule be selected first. Use the radio buttons in the left column to select the desired rule.
Outgoing Rules	
#	For the default rule, this will display "Default". For rules which you create, this will display a radio button which allows you to select the rule.
Enable	Indicates whether or not the rule is currently enabled. For rules you have added, this column will contain a checkbox, allowing you to easily enable or disable the rule. (Click "Save" after making any changes.)
Service Name	The Service covered by this rule.
Action	The action performed on connections which are covered by this rule.
LAN Users	The LAN PC or PCs covered by this rule.
WAN Servers	The WAN IP address or addresses covered by this rule.
Log	Indicates whether or not connections covered by this rule should be logged.
Buttons	Use the *Add* button to create a new rule. The other buttons - *Edit*, *Move*, or *Delete* - require that a rule be selected first. Use the radio buttons in the left column to select the desired rule.

Incoming Rules (Inbound Services)

This screen is displayed when the "Add" or "Edit" button for Incoming Rules is clicked.

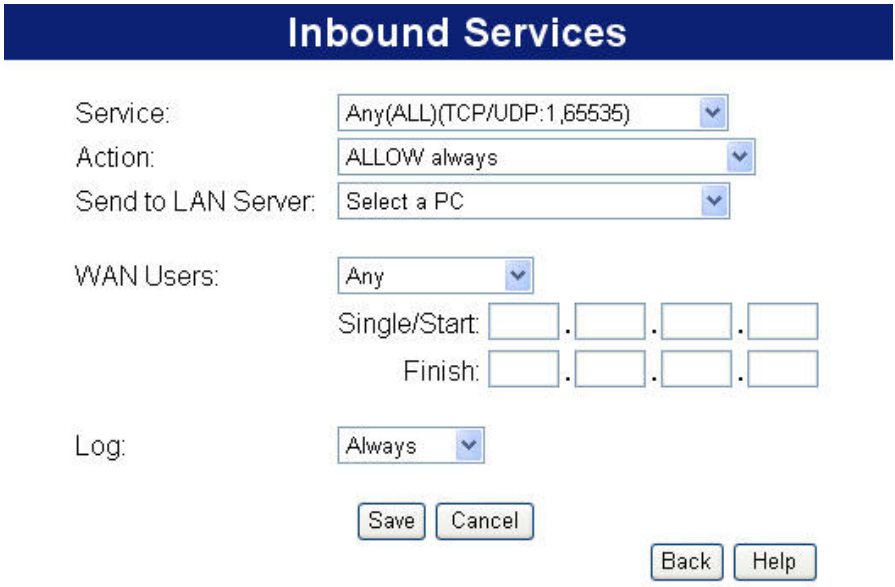

Figure 36: Inbound Services Screen

Data - Incoming Rules Screen

Inbound Services	
Service	Select the desired Service. This determines which packets are covered by this rule. If necessary, you can define a new Service on the "Services" screen, by defining the protocols and port numbers used by the Service.
Action	Select the desired action for packets covered by this rule: • ALLOW always • ALLOW by schedule, otherwise Block • BLOCK always • BLOCK by schedule, otherwise Allow **Note:** • Any inbound traffic which is not allowed by rules you create will be blocked by the Default rule. • BLOCK rules are only useful if the traffic is already covered by an ALLOW rule. (That is, you wish to block a sub-set of traffic which is currently allowed by another rule.) • To define the Schedule used in these selections, use the "Schedule" screen.
Send to LAN Server	Select the PC or Server on your LAN which will receive the inbound traffic covered by this rule.
WAN Users	These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired

	option: • **Any** - All IP addresses are covered by this rule. • **Single address** - Enter the required address in the "Single/Start" fields. • **Address range** - If this option is selected, you must enter the desired values in the "Single/Start" and "Finish" fields to determine the address range.
Log	This determines whether packets covered by this rule are logged. Select the desired action. • **Always** - always log traffic considered by this rule, whether it matches or not. (This is useful when debugging your rules.) • **Never** - never log traffic considered by this rule, whether it matches or not. • **Match** - Log traffic only it matches this rule. (The action is determined by this rule.) • **Not Match** - Log traffic which is considered by this rule, but does not match (The action is NOT determined by this rule.)

Outgoing Rules (Outbound Services)

This screen is displayed when the "Add" or "Edit" button for Outgoing Rules is clicked.

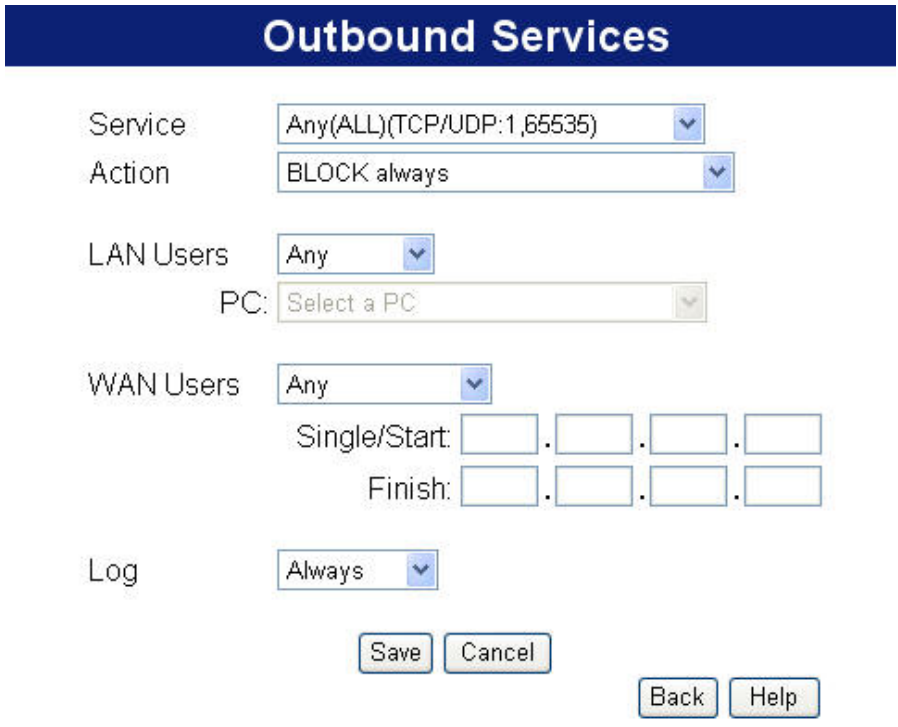

Figure 37: Outbound Services Screen

Data - Outbound Rules Screen

Outbound Services	
Service	Select the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the "Services" menu option
Action	Select the desired action for packets covered by this rule: • BLOCK always • BLOCK by schedule, otherwise Allow • ALLOW always • ALLOW by schedule, otherwise Block **Note:** • Any outbound traffic which is not blocked by rules you create will be allowed by the Default rule. • ALLOW rules are only useful if the traffic is already covered by a BLOCK rule. (That is, you wish to allow a subset of traffic which is currently blocked by another rule.) • To define the Schedule used in these selections, use the "Schedule" screen.
LAN Users	Select the desired option to determine which PCs are covered by this rule: • **Any** - All PCs are covered by this rule. • **Single PC** - Only the selected PC is covered by this rule. If selected, you must select the PC. **PC** - If using Single PC above, select the PC or Server on your LAN which will be covered by this rule.
WAN Users	These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option: • **Any** - All IP addresses are covered by this rule. • **Single address** - Enter the required address in the "Single/Start" fields. • **Address range** - If this option is selected, you must enter the "Start" and "Finish" fields.
Log	This determines whether packets covered by this rule are logged. Select the desired action. • **Always** - always log traffic considered by this rule, whether it matches or not. (This is useful when debugging your rules.) • **Never** - never log traffic considered by this rule, whether it matches or not. • **Match** - Log traffic only it matches this rule. (The action is determined by this rule.) • **Not Match** - Log traffic which is considered by this rule, but does not match (The action is NOT determined by this rule.)

Firewall Services

Services are used when creating Firewall Rules.

If you wish to create a firewall rule, but the required service is not listed in the "Service" list, you can use this feature to define the required service or services. Once created, these services will be listed in the "Service" list, and can be used when creating Firewall Rules.

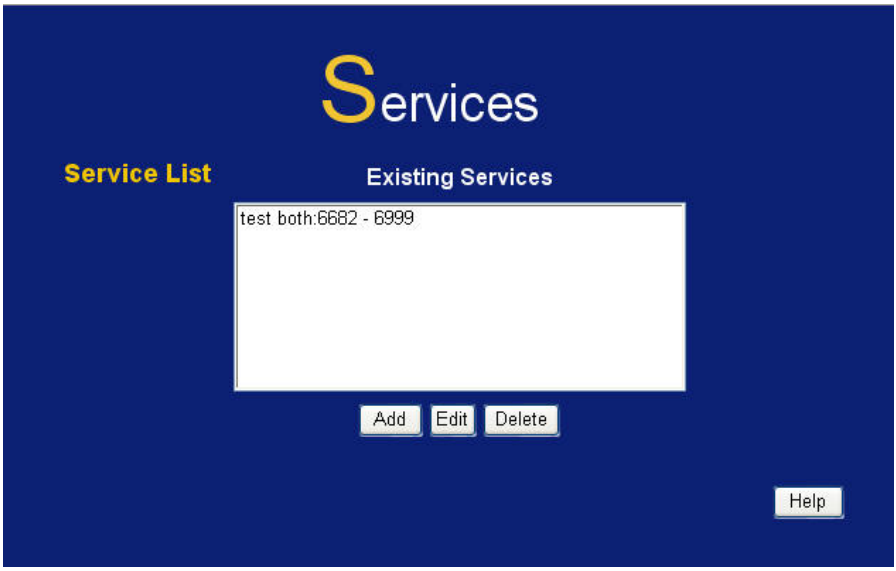

Figure 38: Add Services Screen

Data - Services

Services	
Existing Services	This lists any Services you have defined. If you have not defined any Services, this list will be empty. Once you define some services, they will be listed here, and also shown in the Service list used to create Firewall rules. (User-defined services are at the end of the list, after the pre-defined services.)
Add	Use this to open a sub-screen where you can add a new service.
Edit	To modify a service, select it, and then click this button.
Delete	Use this button to delete the selected service. You can delete any services you have defined.

Virtual Servers

This feature, sometimes called *Port Forwarding*, allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

- Your Server does not have a valid external IP Address.
- Attempts to connect to devices on your LAN are blocked by the firewall in this device.

The "Virtual Server" feature solves these problems and allows Internet users to connect to your servers, as illustrated below.

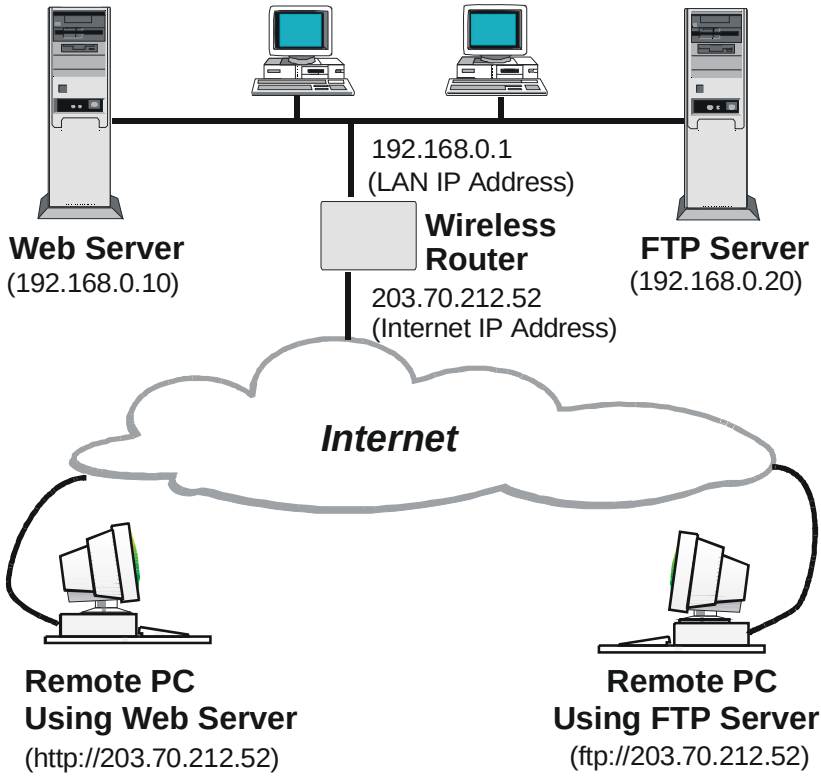

Figure 39: Virtual Servers

IP Address seen by Internet Users

Note that, in this illustration, both Internet users are connecting to the same IP Address, but using different protocols.

To Internet users, all virtual Servers on your LAN have the same IP Address. This IP Address is allocated by your ISP.

This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers.

However, you can use the *DDNS (Dynamic DNS)* feature to allow users to connect to your Virtual Servers using a URL, instead of an IP Address.

Virtual Servers Screen

- The "Virtual Servers" feature allows Internet Users to access PCs on your LAN.
- The PCs must be running the appropriate Server Software.

- For Internet Users, ALL of your Servers have the same IP address. This IP address is allocated by your ISP.
- To make it easier for Internet users to connect to your Servers, you can use the "DDNS" feature. This allows Internet users to connect to your Servers with a URL, rather than an IP address. This technology works even if your ISP allocates dynamic IP addresses (IP address is allocated upon connection, so it may change each time you connect).

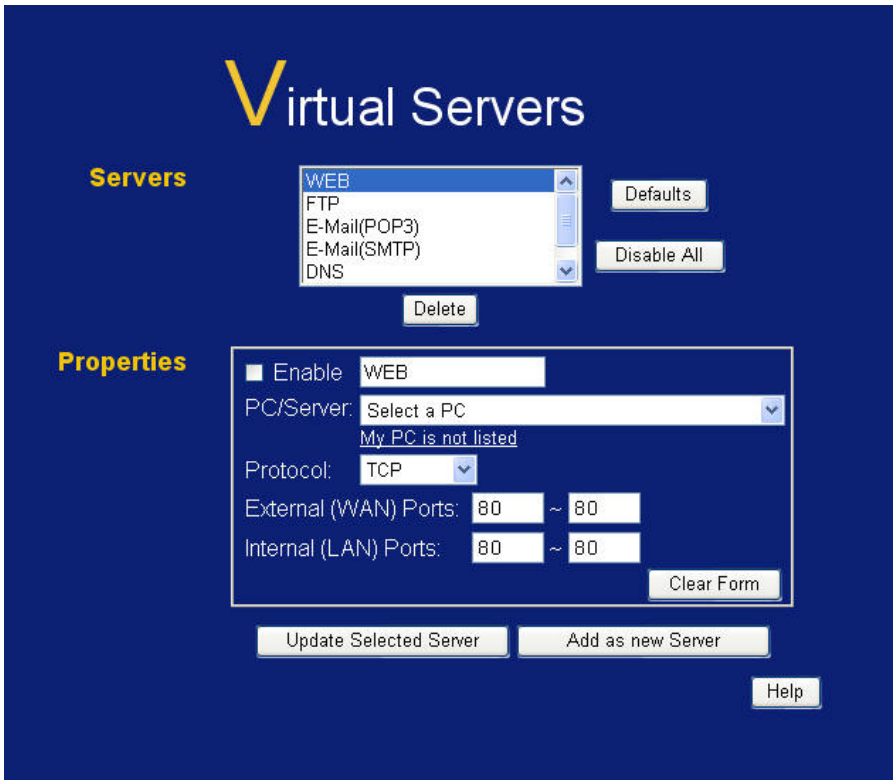

Figure 40: Virtual Servers Screen

Data - Virtual Servers Screen

Servers	
Servers	This lists a number of common Server types. If the desired Server type is not listed, you can create a Firewall Rule to achieve the same effect as the Virtual Server function.
Properties	
Enable	Use this to Enable or Disable support for this Server, as required. If Enabled, you must select the PC to which this traffic will be sent.
PC/Server	Select the PC for this Server. The PC must be running the appropriate Server software.
Protocol	Select the protocol (TCP, UDP, TCP/ UDP) used by the Server.
External Ports	Enter the range of external port numbers.

Internal Ports	Enter the range of internal port numbers.
Buttons	
Defaults	This will delete any Servers you have defined, and set the pre-defined Servers to use their default port numbers.
Disable All	This will cause the "Enable" setting of all Virtual Servers to be set OFF.
Update Selected Server	Update the current Virtual Server entry, using the data shown in the "Properties" area on screen.
Add as new Server	Add a new entry to the Virtual Server list, using the data shown in the "Properties" area on screen. The entry selected in the list is ignored, and has no effect.
Delete	Delete the current Virtual Server entry. Note that the pre-defined Servers can not be deleted. Only Servers you have defined yourself can be deleted.
Clear Form	Clear all data from the "Properties" area, ready for input of a new Virtual Server entry.

For each entry, the PC must be running the appropriate Server software.

Defining your own Virtual Servers

If the type of Server you wish to use is not listed on the *Virtual Servers* screen, you can define and manage your own Servers:

Create a new Server:

1. Click "Clear Form"
2. Enter the required data, as described above.
3. Click "Add".
4. The new Server will now appear in the list.

Modify (Edit) a Server:

1. Select the desired Server from the list
2. Make any desired changes (for example, change the Enable/Disable setting).
3. Click "Update Selected Server" to save changes to the selected Server.

Delete a Server:

1. Select the entry from the list.
2. Click "Delete".

Note: You can only delete Servers you have defined. Pre-defined Server cannot be deleted.

From the Internet, ALL Virtual Servers have the IP Address allocated by your ISP.

Connecting to the Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use the Internet IP Address (the IP Address allocated to you by your ISP).
e.g.

http://203.70.212.52

ftp://203.70.212.52

It is more convenient if you are using a Fixed IP Address from your ISP, rather than Dynamic. However, you can use the *Dynamic DNS* feature to allow users to connect to your Virtual Servers using a URL, rather than an IP Address.

Options

This screen allows advanced users to enter or change a number of settings. For normal operation, there is no need to use this screen or change any settings.

An example ***Options*** screen is shown below.

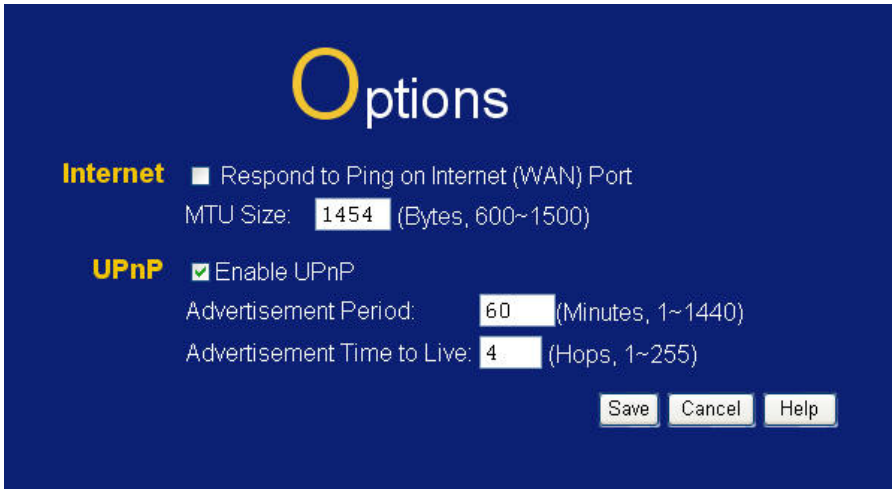

Figure 41: Options Screen

Data - Options Screen

Internet	
Respond to Ping	• If checked, the Wireless Router will respond to Ping (ICMP) packets received from the Internet. • If not checked, Ping (ICMP) packets from the Internet will be ignored. Disabling this option provides a slight increase in security.
MTU Size	Enter a value between 1 and 1500. **Note:** MTU (Maximum Transmission Unit) size should only be changed if advised to do so by Technical Support.
UPnP	
UPnP	• UPnP (Universal Plug and Play) allows automatic discovery and configuration of equipment attached to your LAN. UPnP is by supported Windows ME, XP, or later. • If Enabled, this device will be visible via UPnP. • If Disabled, this device will not be visible via UPnP.
Advertisement Period	Enter the desired value, in minutes. The valid range is from 1 to 1440.
Advertisement Time to Live	Enter the desired value, in hops. The valid range is from 1 to 255.

Port Trigger

This screen can be used for the Port Trigger

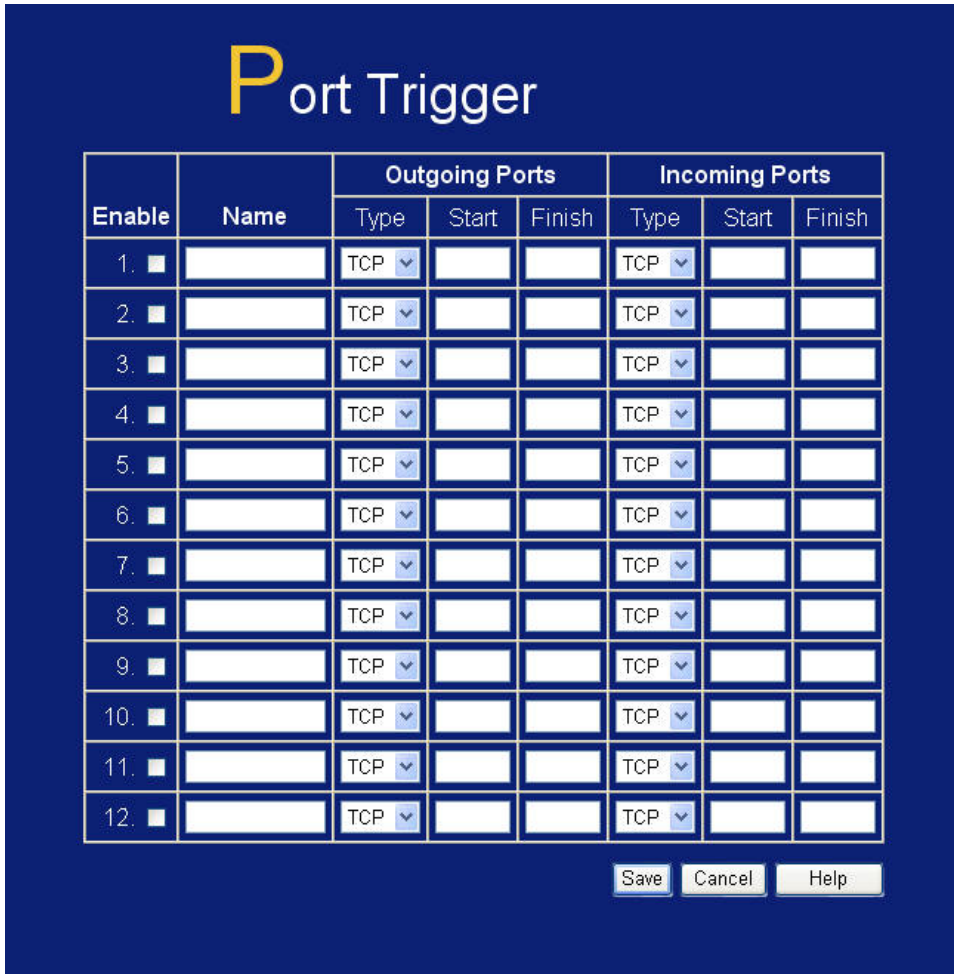

Figure 42: Port Trigger Screen

Schedule

This Schedule can be used for the Firewall Rules and the URL filter.

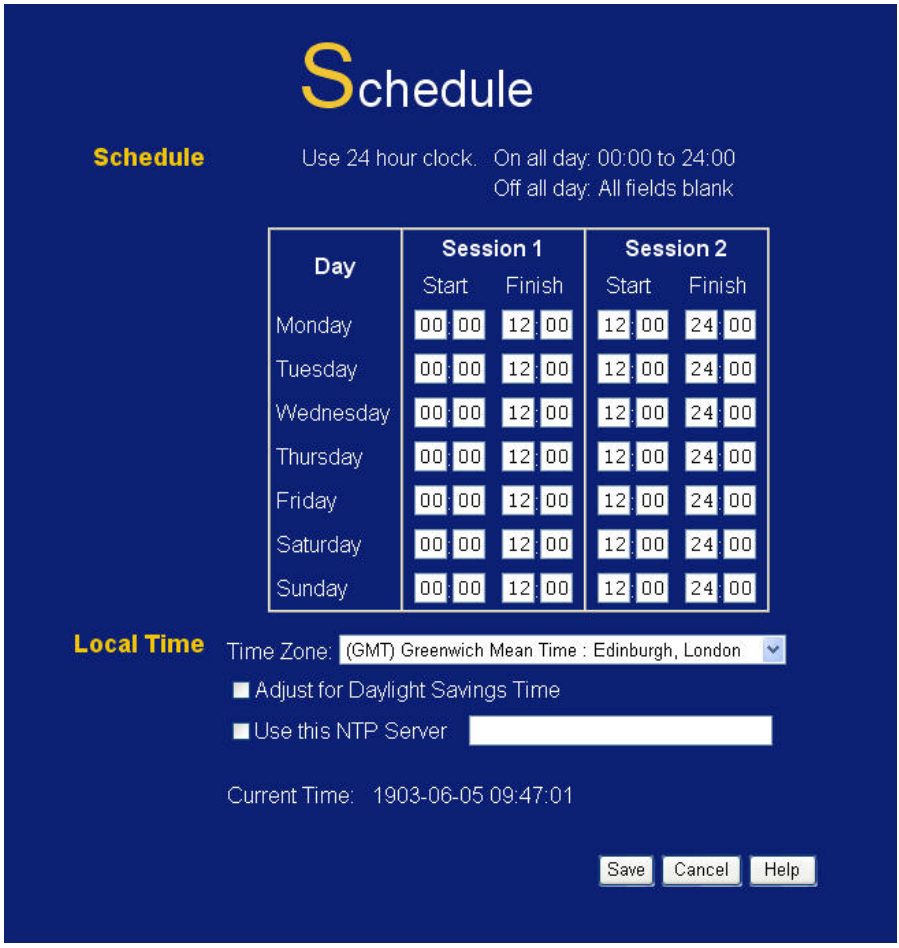

Figure 43: Schedule Screen

Data - Schedule Screen

Schedule	
Day	Each day of the week can scheduled independently.
Session 1 **Session 2**	Two (2) separate sessions or periods can be defined. Session 2 can be left blank if not required.
Start Time	Enter the start using a 24 hr clock.
Finish Time	Enter the finish time using a 24 hr clock.
Local Time	
Time Zone	In order to display your local time correctly, you must select your "Time Zone" from the list.
Adjust for Daylight Savings Time	If your region uses Daylight Savings Time, you must manually check "Adjust for Daylight Savings Time" at the beginning of the adjustment period, and uncheck it at the end of the Daylight Savings period.

Use this NTP Server	If you prefer to use a particular NTP server as the primary NTP server, check the checkbox "Use this NTP Server" and enter the Server's IP address in the fields provided.. If this setting is not enabled, the default NTP Servers are used.
Current Time	This displays the current time on the Wireless Broadband Router, at the time the page is loaded.

Chapter 7
Advanced Administration

This Chapter explains the settings available via the "Administration" section of the menu.

Overview

Normally, it is not necessary to use these screens, or change any settings. These screens and settings are provided to deal with non-standard situations, or to provide additional options for advanced users.

The available settings and features are:

PC Database	This is the list of PCs shown when you select the "DMZ PC" or a "Virtual Server". This database is maintained automatically, but you can add and delete entries for PCs which use a Fixed (Static) IP Address.
Diagnostics	Perform a Ping or DNS Lookup.
Config File	Backup or restore the configuration file for the Wireless Broadband Router. This file contains all the configuration data.
Logs	View or clear all logs, set E-Mailing of log files and alerts.
Remote Admin	Allow settings to be changed from the Internet.
Upgrade Firmware	Upgrade the Firmware (software) installed in your Wireless Broadband Router.

PC Database

This page will list the PC device connect to router.

- It eliminates the need to enter IP addresses.
- Also, you do not need to use fixed IP addresses on your LAN.

PC Database Screen

An example ***PC Database*** screen is shown below.

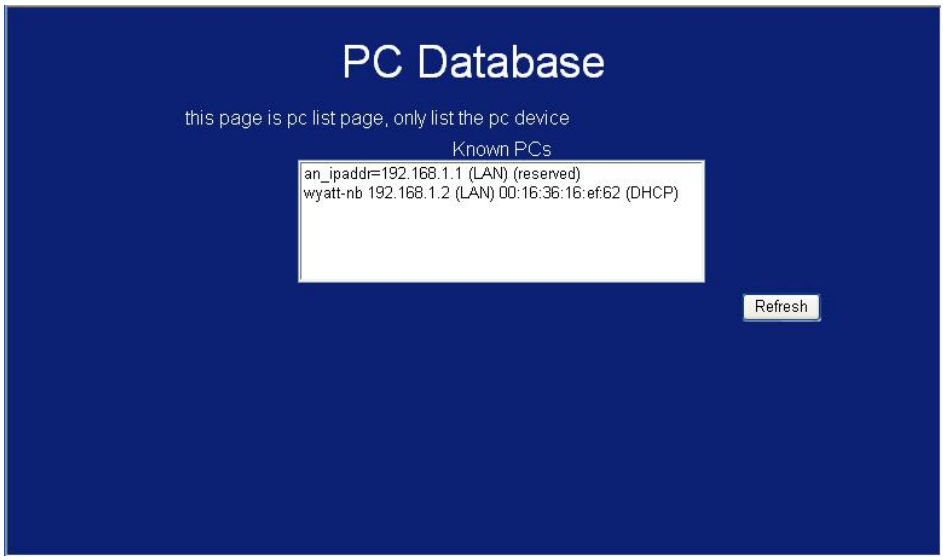
PC Database
this page is pc list page, only list the pc device
Known PCs
an_ipaddr=192.168.1.1 (LAN) (reserved)
wyatt-nb 192.168.1.2 (LAN) 00:16:36:16:ef:62 (DHCP)
Refresh

Figure 44: PC Database

- PCs which are "DHCP Clients" are automatically added to the database, and updated as required.
- By default, non-Server versions of Windows act as "DHCP Clients"; this setting is called "Obtain an IP Address automatically".
- The Wireless Broadband Router uses the "Hardware Address" to identify each PC, not the name or IP address. The "Hardware Address" can only change if you change the PC's network card or adapter.

Data - PC Database Screen

Known PCs	This lists all current entries. Data displayed is *name (IP Address) type*. The "type" indicates whether the PC is connected to the LAN.
Buttons	
Refresh	Update the data on screen.

Diagnostics

This screen allows you to perform a "Ping" or a "DNS lookup". These activities can be useful in solving network problems.

An example ***Network Diagnostics*** screen is shown below.

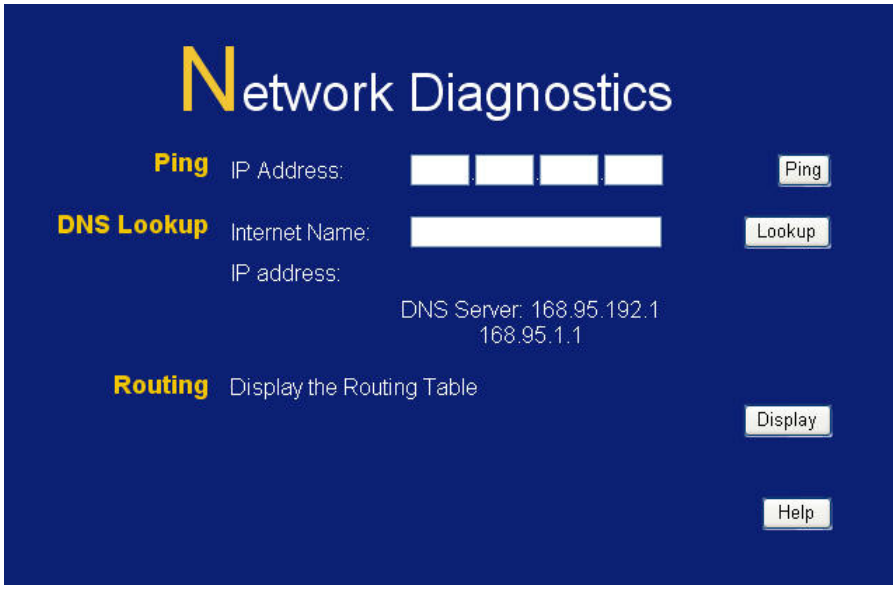

Figure 45: Network Diagnostics Screen

Data - Network Diagnostics Screen

Ping	
Ping this IP Address	Enter the IP address you wish to ping. The IP address can be on your LAN, or on the Internet. Note that if the address is on the Internet, and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.
Ping Button	After entering the IP address, click this button to start the "Ping" procedure. The results will be displayed in the *Ping Results* pane.
DNS Lookup	
Internet name	Enter the Domain name or URL for which you want a DNS (Domain Name Server) lookup. Note that if the address in on the Internet, and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.
Lookup Button	After entering the Domain name/URL, click this button to start the "DNS Lookup" procedure.
Routing	
Display	Click this button to display the internal routing table. This information can be used by Technical Support and other staff who understand Routing Tables.

Config File

This feature allows you to download the current settings from the Wireless Broadband Router, and save them to a file on your PC.

You can restore a previously-downloaded configuration file to the Wireless Broadband Router, by uploading it to the Wireless Broadband Router.

This screen also allows you to set the Wireless Broadband Router back to its factory default configuration. Any existing settings will be deleted.

An example ***Config File*** screen is shown below.

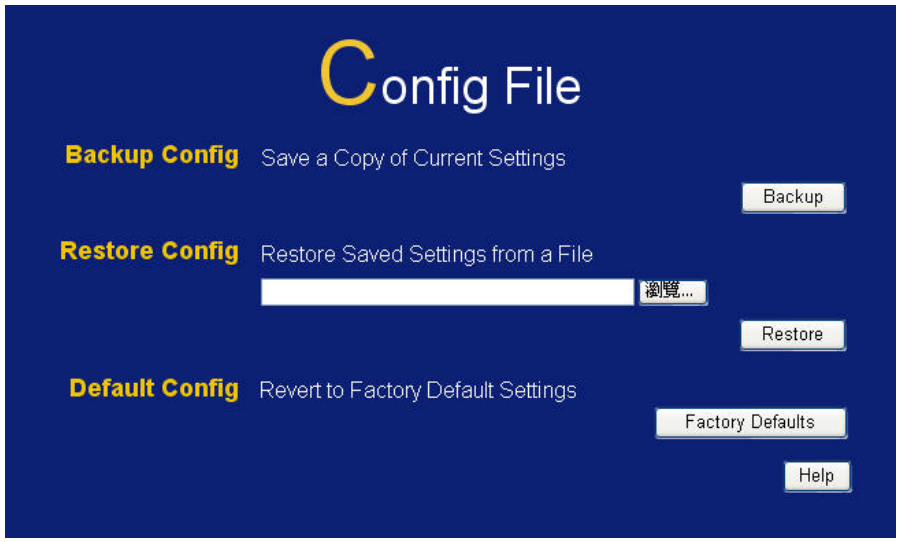

Figure 46: Config File Screen

Data - Config File Screen

Backup Config	Use this to download a copy of the current configuration, and store the file on your PC. Click *Backup* to start the download.
Restore Config	This allows you to restore a previously-saved configuration file back to the Wireless Broadband Router. Click *Browse* to select the configuration file, then click *Restore* to upload the configuration file. **WARNING!** Uploading a configuration file will destroy (overwrite) ALL of the existing settings.
Default Config	Clicking the *Factory Defaults* button will reset the Wireless Broadband Router to its factory default settings. **WARNING!** This will delete ALL of the existing settings.

Logs

The Logs record various types of activity on the Wireless Broadband Router. This data is useful for troubleshooting, but enabling all logs will generate a large amount of data and adversely affect performance.

Logs
Logs
Current time: 1903-06-05 09:49:42
[Dhcp] Fri 1903-06-05 08:11:00 192.168.1.2 0
[Login] Fri 1903-06-05 08:11:26 syslog: [Logi
[Logout] Fri 1903-06-05 08:11:49 syslog: [Log
[Logout] Fri 1903-06-05 08:11:49 syslog: [Log
[Login] Fri 1903-06-05 08:20:09 syslog: [Logi
[Logout] Fri 1903-06-05 08:20:18 syslog: [Log
[Bootup] Fri 1903-06-05 08:20:28 - Router sta
[Dhcp] Fri 1903-06-05 08:20:44 192.168.1.2 0
[Wan] Fri 1903-06-05 08:22:01 WAN DHCP Client
[Login] Fri 1903-06-05 08:25:22 syslog: [Logi
[Logout] Fri 1903-06-05 08:47:56 syslog: [Log
[Login] Fri 1903-06-05 08:47:59 syslog: [Logi
Refresh
Clear Log
Send Log
Include in Log
Attempted access to blocked sites
Connections to the Web-based interface of this Router
Router operation (start up, get time etc)
Known DoS attacks and Port Scans
Syslog
Disable
Broadcast on LAN
Send to this Syslog Server:
Save
Cancel
Help

Figure 47: Logs Screen

Data - Logs Screen

Logs	
Current Time	The current time on the Wireless Broadband Router is displayed.
Log Data	Current log data is displayed in this panel.
Refresh Button	Use this button to update the log data.

Remote Administration

If enabled, this feature allows you to manage the Wireless Broadband Router via the Internet.

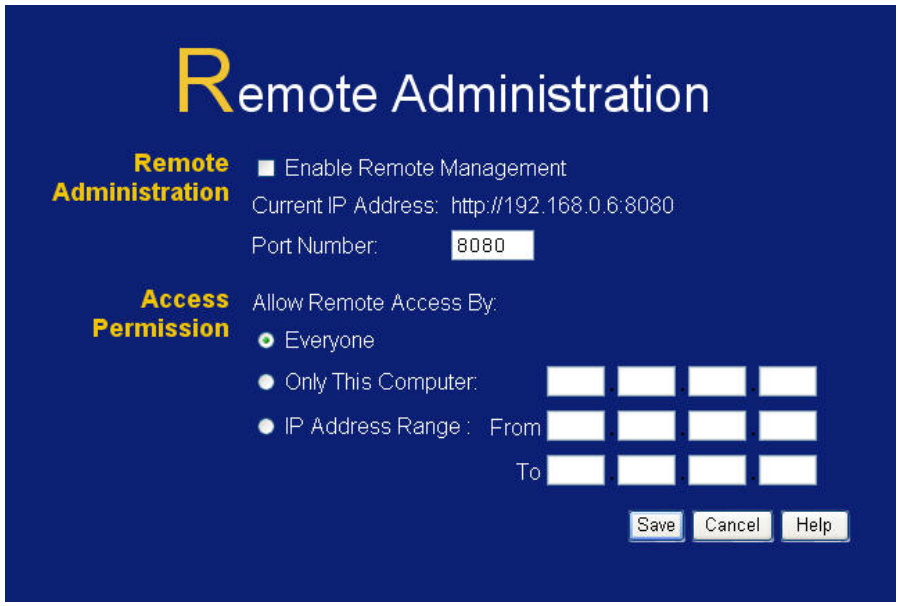

Figure 48: Remote Administration Screen

Data - Remote Administration Screen

Remote Administration	
Enable Remote Management	Check to allow administration/management via the Internet. (To connect, see below). If Disabled, this device will ignore Administration connection attempts from the Internet.
Current IP Address	This is the current address you will use when accessing this device from the Internet. To connect, see details and an example below.
Port Number	Enter a port number between 1 and 65535. The default for HTTP (Web) connections is port 80, but using port 80 will prevent the use of a Web "Virtual Server" on your LAN. So using a different port number is recommended. The default value is 8080. The port number must be specified in your Browser when you connect. See the following section for details.

To connect from a remote PC via the Internet

1. Ensure your Internet connection is established, and start your Web Browser.
2. In the "Address" bar, enter "HTTP://" followed by the Internet IP Address of the Wireless Broadband Router. If the port number is not 80, the port number is also required. (After the IP Address, enter ":" followed by the port number.)
   e.g.

HTTP://123.123.123.123:8080y

This example assumes the WAN IP Address is 123.123.123.123, and the port number is 8080.

3. You will then be prompted for the login name and password for this device.

Upgrade Firmware

The firmware (software) in the Wireless Broadband Router can be upgraded using your Web Browser.

You must first download the upgrade file, then select *Upgrade Firmware* on the *Administration* menu. You will see a screen like the following.

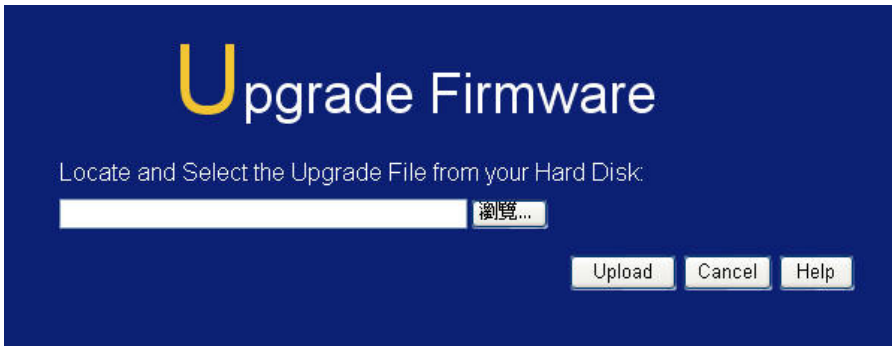

Figure 49: Router Upgrade Screen

To perform the Firmware Upgrade:

1. Click the *Browse* button and navigate to the location of the upgrade file.
2. Select the upgrade file. Its name will appear in the *Upgrade File* field.
3. Click the *Upload* button to commence the firmware upgrade.

The Wireless Broadband Router is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the Wireless Broadband Router will be lost.

Appendix A
Troubleshooting

This Appendix covers the most likely problems and their solutions.

Overview

This chapter covers some common problems that may be encountered while using the Wireless Broadband Router and some possible solutions to them. If you follow the suggested steps and the Wireless Broadband Router still does not function properly, contact your dealer for further advice.

General Problems

Problem 1: **Can't connect to the Wireless Broadband Router to configure it.**

Solution 1: Check the following:

- The Wireless Broadband Router is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the Wireless Broadband Router are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.0.2 to 192.168.0.254 and thus compatible with the Wireless Broadband Router's default IP Address of 192.168.0.1.
  Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Broadband Router.
  In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Internet Access

Problem 1: **When I enter a URL or IP address I get a time out error.**

Solution 1: A number of things could be causing this. Try the following troubleshooting steps.

- Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address.
- If the PCs are configured correctly, but still not working, check the Wireless Broadband Router. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)
- Check the Wireless Broadband Router's status screen to see if it is working correctly.

Problem 2: **Some applications do not run properly when using the Wireless Broadband Router.**

Solution 2: The Wireless Broadband Router processes the data passing through it, so it is not transparent.

For incoming connections, you must use the Virtual Server or Firewall Rules to specify the PC which will receive the incoming traffic.

You can also use the *DMZ* function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.

Wireless Access

Problem 1: **My PC can't locate the Wireless Access Point.**

Solution 1: Check the following.

- Your PC is set to *Infrastructure Mode*. (Access Points are always in *Infrastructure Mode*)
- The SSID on your PC and the Wireless Access Point are the same.
  Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup".
- Both your PC and the Wireless Broadband Router must have the same setting for WEP. The default setting for the Wireless Broadband Router is disabled, so your wireless station should also have WEP disabled.
- If WEP is enabled on the Wireless Broadband Router, your PC must have WEP enabled, and the key must match.
- If the Wireless Broadband Router's *Wireless* screen is set to *Allow*, then each of your Wireless stations must have been designated as "Trusted", or the Wireless station will be blocked.
- To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Broadband Router. Remember that the connection range can be as little as 100 feet in poor environments.

Problem 2: **Wireless connection speed is very slow.**

Solution 2: The wireless system will connect at the highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with the following:

- Wireless Broadband Router location.
  Try adjusting the location and orientation of the Wireless Broadband Router.
- Wireless Channel
  If interference is the problem, changing to another channel may show a marked improvement.
- Radio Interference
  Other devices may be causing interference. You can experiment by switching other devices Off, and see if this helps. Any "noisy"

devices should be shielded or relocated.

- RF Shielding
  Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Wireless Broadband Router.

Appendix B
About Wireless LANs

This Appendix provides some background information about using Wireless LANs (WLANs).

Modes

Infrastructure Mode

In Infrastructure Mode, one or more Access Points are used to connect Wireless Stations (e.g. Notebook PCs with wireless cards) to a wired (Ethernet) LAN. The Wireless Stations can then access all LAN resources.

Access Points can only function in "Infrastructure" mode, and can communicate only with Wireless Stations which are set to "Infrastructure" mode.

BSS/ESS

BSS

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other.

ESS

A group of Wireless Stations, and multiple Access Points, all using the same ID (ESSID), form an Extended Service Set (ESS).

Different Access Points within an ESS can use different Channels. In fact, to reduce interference, it is recommended that adjacent Access Points SHOULD use different channels.

As Wireless Stations are physically moved through the area covered by an ESS, they will automatically change to the Access Point which has the least interference or best performance. This capability is called **Roaming**. (Access Points do not have or require Roaming capabilities.)

Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available. If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference.

- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)
- If using "Ad-hoc" mode (no Access Point), all Wireless stations should be set to use the same Channel. However, most Wireless stations will still scan all Channels to see if there is an existing "Ad-hoc" group they can join.

WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted.

This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

If WEP is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WEP	Off, 64 Bit, 128 Bit
Key	For 64 Bit encryption, the Key value must match. For 128 Bit encryption, the Key value must match
WEP Authentication	Open System or Shared Key.

WPA-PSK

WPA-PSK is another standard for encrypting data before it is transmitted. This is a later standard than WEP (Wired Equivalent Privacy), and provides greater security for your data. Data is encrypted using a key which is automatically generated and changed often.

If all your Wireless stations support WPA-PSK, you should use this instead of WEP.

If WPA-PSK is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WPA PSK (Pre-shared Key)	Enter the same value on every station and the AP. The PSK must be from 8 to 63 characters in length. The key used for the actual encryption is derived from this key.
Encryption	The same encryption method must be used. The most common encryption method is TKIP. Another widely-supported method is AES.

Wireless LAN Configuration

To allow Wireless Stations to use the Access Point, the Wireless Stations and the Access Point must use the same settings, as follows:

Mode	On client Wireless Stations, the mode must be set to "Infrastructure".

	(The Access Point is always in "Infrastructure" mode.)
SSID (ESSID)	Wireless Stations should use the same SSID (ESSID) as the Access Point they wish to connect to. Alternatively, the SSID can be set to "any" or null (blank) to allow connection to any Access Point.
Wireless Security	The Wireless Stations and the Access Point must use the same settings for Wireless security. (None, WEP, WPA-PSK). **WEP:** If WEP is used, the Key size (64Bit, 128Bit), Key value, and Authentication settings must be the same on the Wireless Stations and the Access Point. **WPA-PSK:** If WPA-PSK is used, all Wireless Stations must be set to use WPA-PSK, and have the same Pre-shared Key and encryption system. For **Ad-hoc networks** (no Access Point), all Wireless stations must use the same security settings.

Appendix C
Specifications

Multi-Function Wireless Broadband Router

Model	LevelOne WBR-6000 *N_One* Wireless Broadband Router
Dimensions	173mm(W) * 147mm(D) * 37mm(H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	4 * 10/100BaseT (RJ45) LAN connection 1 * RJ11 for WAN connection
LEDs	6
Power Adapter	12VDC 1A External

Wireless Interface

Standards	IEEE802.11b, IEEE802.11g WLAN, 802.11n Draft
Frequency	2.4 to 2.4835GHz (Industrial Scientific Medical Band)
Channels	Maximum 14 Channels, depending on regulatory authorities
Modulation	CCK, DQPSK, DBPSK, OFDM/CCK
Data Rate	Up to 300 Mbps (802.11n Draft)
Security	WEP 64Bit, 128Bit, WPA-PSK,WPA2-PSK, MAC address checking
Output Power	13dBm (typical)

Regulatory Approvals

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

CE Approval

CE Standards

This product complies with the 99/5/EEC directives, including the following safety and EMC standards:

- EN300328-2
- EN301489-1/-17
- EN60950

CE Marking Warning

This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Hereby, Digital Data Communications, declares that this (Model-no. WBR-6000) is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The CE-Declaration of Conformity can be downloaded at:

http://www.levelone.eu/support.php